CASO PEGASUS: VULNERACIONES DE LOS DERECHOS A LA INTIMIDAD, LA DEFENSA Y OTROS DERECHOS

SÍNDIC
EL DEFENSOR DE LES PERSONES

CASO PEGASUS: VULNERACIONES DE LOS DERECHOS A LA INTIMIDAD, LA DEFENSA Y OTROS DERECHOS

SÍNDIC
EL DEFENSOR DE LES PERSONES

Síndic de Greuges de Cataluña

1ª edición: Junio 2022
Caso Pegasus: vulneraciones de los derechos a la intimidad, la defensa y otros derechos. Junio 2022
Maquetación: Síndic de Greuges
Foto de cubierta: (c) Pixabay

ÍNDICE

INTRODUCCIÓN

A mediados de abril de 2022, la revista The New Yorker se hacía eco de un informe elaborado por Citizen Lab, de la Munk School of Global Affairs & Public Policy de la Universidad de Toronto (Canadà). El informe ponía de manifiesto que personas del entorno político y social independentista habían sido objeto de espionaje con *malware* como Pegasus y Candiru, al menos desde 2015. El periódico *The Guardian* también se había hecho eco de estos informes ya en 2020 y Amnistía Internacional había elaborado un informe técnico el año 2021.[1]

Según estas publicaciones, más de sesenta personas entre cargos políticos, abogados y personas relacionadas con el movimiento independentista catalán fueron objetivo del sistema de ciberespionaje Pegasus, instalado en sus terminales móviles. Estos datos técnicos han sido parcialmente confirmados por el Centro Nacional de Inteligencia (CNI), que admite haber investigado con este sistema a dieciocho personas, con la correspondiente autorización judicial. En trece de estos casos se utilizó el sistema Pegasus.

Si bien la existencia de Pegasus se conoce desde hace años, existen algunos factores clave que aumentan sensiblemente la preocupación actual: en primer lugar, España es el primer caso en el que un gobierno europeo admite el uso de este tipo de sistemas y, en segundo lugar, los objetivos de la investigación son cargos políticos electos de alto nivel, como el expresidente del Parlamento catalán Roger Torrent o el actual presidente de la Generalitat, Pere Aragonès. Además, las nuevas noticias de casos en Polonia, Hungría, Alemania y Bélgica ponen de manifiesto el uso común de herramientas de ciberespionaje dentro de la Unión Europea. El último giro de la historia ha sido el descubrimiento de que altos cargos del gobierno español (el presidente, Pedro Sánchez, y la ministra de Defensa, Margarita Robles) también han sido espiados con el propio sistema Pegasus.

El Síndic de Greuges de Cataluña tiene la función de proteger y salvaguardar los derechos fundamentales de los ciudadanos de Cataluña cuando esos derechos están en peligro por acciones de la Administración. El informe del Citizen Lab pone de manifiesto un espionaje masivo a ciudadanos catalanes vinculados a tesis independentistas o a personas relacionadas con estos ciudadanos, así como a su defensa jurídica. Evidencia asimismo que este seguimiento se ha llevado a cabo mediante la instalación clandestina en sus teléfonos móviles de un programa oculto elaborado por la empresa israelí NSO Group.

A raíz de estos acontecimientos, se pusieron en marcha determinados mecanismos institucionales y el 4 de mayo de 2022 se constituyó la Comisión de Secretos Oficiales del Congreso de Diputados (después de tres años de legislatura) y compareció quien entonces era la directora del CNI. De su comparecencia se pudo concluir que dieciocho personalidades catalanas, vinculadas a planteamientos independentistas y en buena medida sin diligencias penales abiertas en su contra, fueron monitorizadas por el CNI entre diciembre de 2019 y el primer semestre de 2020. Según relató la ya exdirectora del CNI, todos los seguimientos tenían autorización judicial y seguían la Directiva de inteligencia que emitió el gobierno español en 2019.

Cabe recordar que esta directiva es secreta, como lo son las actividades del CNI –incluidas las peticiones al magistrado del Tribunal Supremo que debe autorizar las intervenciones que afectan a derechos fundamentales de los ciudadanos a investigar–, y como lo son, asimismo, sus resoluciones. Por lo que respecta a las sesiones de la Comisión de Secretos Oficiales del Congreso de Diputados, también son secretas.

En mayo de 2020 el Síndic de Greuges abrió una primera actuación de oficio sobre el presunto espionaje del entonces presidente del Parlamento catalán, Roger Torrent. El documento se dirigió a la Agencia de Ciberseguridad de Cataluña, que informó de que tras investigar el posible compromiso de los terminales por el *malware* Pegasus, los resultados no eran concluyentes.

[1] Aparte del informe, es conveniente consultar también su apendice D y el apendice E.

Sin embargo, el 19 de abril de 2022, ante las nuevas informaciones publicadas y el alcance que tuvieron, el Síndic abrió una nueva actuación que trasladó al Defensor del Pueblo, como institución constitucional encargada de velar por los derechos frente a todas las administraciones del Estado, incluido, por tanto, el CNI. El Defensor del Pueblo, que ha tenido acceso a todas las autorizaciones judiciales relativas al espionaje de las dieciocho personas mencionadas, ha concluido su investigación con la resolución de 18 de mayo de 2022. También es interesante mencionar el reciente informe de Amnistía Internacional *Pegasus: denuncias de vigilancia masiva en España*.

A partir del informe de Citizen Lab, las referencias en los medios de comunicación, las intervenciones parlamentarias, las comparecencias de altos cargos públicos del gobierno central y el informe del Defensor del Pueblo, el Síndic se encuentra en disposición de presentar un breve informe institucional que analiza el impacto sobre los derechos fundamentales de una intervención como la que permite un *software* malicioso como Pegasus y Candiru. El informe está dividido en dos partes: la primera, de carácter técnico, expone las características tecnológicas y el funcionamiento de estos programas, y la segunda se centra en cómo estos programas pueden afectar a los derechos fundamentales.[2]

[1] Para la primera parte, el Síndic ha contado con la colaboración de la empresa Evidentia, especializada en peritaje informático y para la segunda, ha contado con la participación del profesor Joan J. Queralt, catedrático de Derecho Penal de la Universidad de Barcelona.

I. CIBERESPIONAJE: CONSIDERACIONES TECNOLÓGICAS PARA LA CIUDADANÍA

1. TIPO DE SISTEMAS DE CONTROL, MONITORIZACIÓN Y ESPIONAJE

El objetivo de los sistemas de ciberespionaje como Pegasus es acceder a información confidencial e íntima y a comunicaciones realizadas con dispositivos informáticos. Entre todos los dispositivos informáticos de organizaciones empresariales y personales, lo que contiene más información sensible es el teléfono móvil.

Desde la aparición de los teléfonos inteligentes, y con la enorme popularización de los teléfonos iPhone (Apple) y de los que están basados en Android, las personas almacenamos enormes cantidades de información personal, tales como fotografías, vídeos, documentos, correos electrónicos, mensajería electrónica, historial de navegación en Internet, aplicaciones, etcétera. Además, estos dispositivos integran videocámaras y micrófonos, que pueden ser activados o desactivados por aplicaciones y por el sistema operativo del terminal, y sistemas de geoposición basados en GPS, redes wifi, telefonía móvil e incluso Bluetooth.

Los terminales móviles son, sin duda alguna, el primer objeto de la historia de la humanidad que lo sabe casi todo sobre nosotros, y siempre los llevamos encima. Por este motivo, la información que contienen es preciada por empresas, organizaciones y personas.

Es importante entender que el control o la monitorización de un terminal móvil no siempre es ilegal o no consentido. Todo el mundo está siendo monitoreado de alguna manera en cualquier momento. Por ejemplo, la red de telefonía debe saber dónde está el terminal móvil en cada momento para dirigirle las llamadas, y la ley obliga a los operadores de telefonía a guardar y hacer disponible esa información para las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), siempre con la tutela judicial correspondiente, a fin de investigar casos penales de consideración grave.

Con la misma motivación, la ley también obliga a las empresas proveedoras de servicios digitales a guardar los datos de acceso de sus clientes y usuarios durante un año. Por ello, los proveedores de correo electrónico o de páginas web deben almacenar información susceptible de identificar a las personas que utilizan sus servicios.

En el mundo laboral, está muy bien regulado el uso de la geoposición GPS para conocer la posición de trabajadores que hacen ciertas tareas, incluso utilizando los servicios de geoposición de los terminales móviles corporativos. La actual jurisprudencia permite que, en ciertas condiciones, la empresa controle las herramientas informáticas, incluido el correo electrónico, para garantizar la política de seguridad corporativa. También ha habido sentencias recientes que han legitimado, en ciertas condiciones, el uso de programas que hacen capturas de pantalla de los ordenadores del personal. Ahora bien, esto no significa que todos estos productos informáticos sean legales en España.

La gran diferencia entre estos sistemas comerciales y sistemas como Pegasus es que los productos comerciales normalmente requieren acceso físico al terminal móvil o al ordenador (o a la red local que utilice), y es necesario conocer el PIN de acceso o la contraseña administrativa. Es decir, es muy difícil que puedan ser utilizados por personas que no pertenezcan a un círculo muy cercano a la víctima.

Es muy importante entender que, en condiciones normales, es muy improbable que un ciudadano medio pueda ser espiado por un vecino, una persona conocida, la expareja, un compañero de trabajo, etcétera. Además, la gran mayoría de sistemas operativos de ordenadores y teléfonos móviles incorporan medidas para evitar que puedan instalarse o que puedan utilizarse programas ocultos para el usuario.

Es muy complicado instalar y gestionar un sistema de ciberespionaje en un ordenador o teléfono remoto sin autorización del propietario y de modo que su funcionamiento sea secreto (o no detectable), ya que requiere un conocimiento elevado de la tecnología y recursos técnicos muy avanzados. Por ende, este tipo de sistemas, incluido Pegasus, solo están al alcance de gobiernos, agencias de seguridad o inteligencia o fuerzas y cuerpos de seguridad.

La conclusión de este apartado es que el ciudadano medio no debe temer ser espiado por un sistema de ciberespionaje como Pegasus, y que deben conocerse los diferentes tipos de monitorización de un terminal móvil y cómo se pueden producir (autorizados y no autorizados). La inquietud que ha causado que se hable de Pegasus en los periódicos debe servir para que se haga un control del uso de estas potentes herramientas tecnológicas contra los cargos políticos electos y contra la ciudadanía en general.

2. FUNCIONAMIENTO TECNOLÓGICO DE LOS PROGRAMAS DE CIBERESPIONAJE

Todos los sistemas de monitorización, control o espionaje comparten una base tecnológica, y la diferencia radica en cómo se implementa cada parte. A continuación, se hace una descripción de las fases comunes del ciclo de vida de una solución tecnológica de control informático, y se detallan las características de sistemas de ciberespionaje como Pegasus.

2.1. Fase de localización del objetivo

Esta fase consiste en conocer, por ejemplo, el número de teléfono de la persona objeto del control informático. El dato concreto depende del vector de ataque, y en algunos casos es importante conocer otros datos, tales como direcciones de correo electrónico, tipos de terminal (incluida la versión) o la existencia de otros terminales de la persona.

En escenarios corporativos, con sistemas de monitorización legales, esta localización es trivial y no requiere ningún esfuerzo por parte de la persona que desea instalar el *software*. Ahora bien, en casos de ciberespionaje, esta localización no sería tan trivial y podría requerir tareas y fuentes de información solo al alcance de agencias de inteligencia o cuerpos policiales. Por ejemplo, se sabe que el expresidente de la Generalitat Carles Puigdemont utilizaba un teléfono móvil que no era un teléfono inteligente, lo que imposibilitó la instalación de Pegasus. Según se ha publicado, ante esta problemática, el atacante optó por infectar y controlar a personas de su entorno.

2.2. Fase de infección o instalación del programa

La naturaleza de esta fase depende en gran medida de cada caso.

En casos corporativos, la dirección de la empresa delega esta labor en el departamento de informática, que tiene el control de todo el parque informático, normalmente ordenadores y teléfonos móviles corporativos, por lo que la labor de instalación es trivial, ya sea de forma remota o presencial (la persona empleada lleva el dispositivo al departamento de informática).

Es importante tener en cuenta que no todas las instalaciones de las empresas son legales o están autorizadas. El carácter legal del uso de estas soluciones en ámbito laboral no es objeto de este informe, pero, como consideración general, la empresa debe avisar al personal de su potestad de control, y debe emplear herramientas tecnológicas proporcionales al objetivo perseguido. Los controles de geoposición o pantalla indiscriminados y ocultos suelen considerarse ilegales.

Es importante entender que, sin un acceso físico, y sin conocer las credenciales de acceso, es casi imposible comprometer un ordenador o un teléfono con medios domésticos. Además, fabricantes como Apple o Google llevan un estricto control de las aplicaciones disponibles en sus mercados web (App Store y Google Play) y no permiten aplicaciones de ciberespionaje.

Sin embargo, en casos de ciberespionaje y sistemas como Pegasus, la historia es muy diferente. Empresas como NSO Group provienen del mundo de la seguridad informática o del mundo de la ciberinteligencia, y tienen acceso a información sobre los terminales móviles que ni sus fabricantes conocen.

Se sabe que el sistema Pegasus aprovecha agujeros de seguridad que los fabricantes de los terminales móviles desconocen –y que, por tanto, no están solucionados (estos agujeros se conocen como *vulnerabilidades de día cero* o *zero-day*)– para ejecutar programas informáticos que realizan acciones no permitidas. Es decir, ejecutan programas

que sortean las medidas de seguridad de los teléfonos de Apple o Android.

Las investigaciones hechas por Citizen Lab y Amnistía Internacional revelan que NSO utilizó diferentes vulnerabilidades no conocidas de WhatsApp (Android) e iMessage, FaceTime o iTunes (Apple) para ejecutar código informático no autorizado.

Se conocen tres métodos de ataque: en el primero, el atacante envía un mensaje a la víctima con la intención de convencerla de que haga clic en un enlace. Para engañar a la víctima, se han utilizado mensajes muy personalizados, como avisos de Correos para recoger un paquete, de la Agencia Tributaria, del Registro Mercantil, o incluso enlaces con supuestas noticias de Twitter.

Según este primer método, cuando el usuario hace clic en el enlace, se le dirige a un sitio de Internet falso que descarga un programa informático en su dispositivo y, aprovechando un problema de seguridad de algún componente del terminal, ejecuta código sin limitaciones de seguridad.

En el segundo método, se intercepta la navegación en Internet del terminal, ya sea capturando el tráfico en el sistema de telefonía o mediante un dispositivo que emula ser una torre de telefonía (y hace que el terminal se conecte). Cuando la víctima entra en un sitio de Internet no cifrado (sin protocolo SSL), el atacante inyecta el *malware* que, como en el primer método, aprovecha una vulnerabilidad no conocida para acceder al teléfono.

El tercer método es el más efectivo y utiliza un problema de seguridad que se puede aprovechar sin intervención del usuario. Es el método conocido como *zero-click*. Se sabe que Pegasus, entre 2019 y 2021, podía ser instalado en ciertos teléfonos Apple sin intervención alguna del usuario, aprovechando vulnerabilidades de las aplicaciones iMessage y FaceTime: el atacante enviaba una notificación al teléfono con un contenido malicioso que permitía ejecutar código sin limitaciones de seguridad.

Cuando un teléfono es infectado de una de estas formas, el *malware* descarga e instala el sistema Pegasus propiamente dicho, lo que se conoce como *sistema de mando y control* (*Command & Control* o C&C), que es un programa informático que, de forma oculta, espera órdenes del atacante; por ejemplo, encender el micrófono o enviar los SMS recibidos.

2.3. Ocultación y persistencia

Los sistemas de ciberespionaje como Pegasus tienen la capacidad de ocultarse del sistema operativo y de los usuarios. Normalmente, procuran dejar las mínimas "huellas", por dos razones: la primera, para no ser descubiertos por los usuarios, y la segunda, para no ser descubiertos por analistas de seguridad y expertos en informática forense.

Efectivamente, cuando un virus, un troyano o un sistema de ciberespionaje es descubierto, se suceden una cadena de eventos que normalmente terminan con el negocio del fabricante del sistema malicioso. Se descubren las vulnerabilidades que permiten la infección inicial e instalación del C&C, y normalmente se comunican al fabricante del sistema operativo o de la aplicación de forma privada para que solucione el problema y actualice todos los dispositivos.

Así ocurrió con Pegasus. WhatsApp descubrió que tenía a 14.000 usuarios de su sistema infectados por un programa malicioso que, tras las investigaciones de Citizen Lab y Amnistía Internacional, se identificó como Pegasus. WhatsApp solucionó el problema, lo comunicó a los 14.000 usuarios e inició un proceso de denuncia contra NSO Group que en el momento de redactar este informe todavía está abierto en el Tribunal de Distrito de Estados Unidos para el Distrito Norte de California. Esto también ocurrió con las vulnerabilidades de iMessage, que se comunicaron a Apple y se solucionaron antes de hacerlas públicas.

Normalmente, la publicación y solución de la vulnerabilidad que permite la infección termina con el producto de ciberespionaje . Pero NSO Group ha ido encontrando nuevas vías de infección (lo que se conoce como *nuevos vectores de ataque*). De hecho, se han documentado varias vías de infección distintas entre 2015 y 2021.

Para los programas de espionaje es vital la persistencia, que es la capacidad del programa

informático malicioso de continuar en el dispositivo infectado tras reiniciarlo o apagarlo. Se sabe que Pegasus no se guarda en la memoria no volátil del teléfono, a fin de minimizar su huella y su probabilidad de detección. Cuando el sistema se reinicia, Pegasus pierde su persistencia y es necesaria una nueva infección. Este inconveniente, sin embargo, no es muy importante en terminales móviles porque apenas se apagan ni se reinician.

2.4. Envío de información

Un aspecto clave de los sistemas de ciberespionaje es la comunicación con el atacante: el atacante debe ejecutar órdenes y recibir la información de retorno del sistema infectado.

Actualmente, casi ningún producto de control remoto informático hace conexiones directas entre la persona que controla y el dispositivo controlado, sino que utilizan conexiones a unos servidores centrales que gestionan sus interacciones y gestiones. De esta forma es más fácil evitar medidas de seguridad básicas como cortafuegos, porque suelen configurarse para filtrar el tráfico de datos desde Internet a la red interna, pero no suelen filtrar las conexiones desde la red interna a Internet. Muchas aplicaciones legales y comunes utilizan esta estrategia.

Las aplicaciones de control remoto o monitorización sencillas o legales utilizan, normalmente, una red de servidores intermedios propios del fabricante del programa que son fácilmente identificables. En estos casos, si se investiga el tráfico de datos que genera el sistema de control, es posible identificar el tipo de *software* y su fabricante, aunque no puede identificarse, generalmente, a la persona u organización que está controlando el dispositivo.

En cambio, sistemas como Pegasus utilizan una estrategia más compleja. Para empezar, se cree que utilizan un conjunto de servidores intermedios para cada cliente de Pegasus. De esta forma se aseguran de que un cliente no pueda comprometer la información de otro del mismo servidor ni acceder a él.

Además, se ha comprobado que NSO Group ha aplicado medidas para dificultar la identificación de sus servidores intermedios. Es decir, el análisis de un terminal móvil permite identificar el servidor intermedio con el que se comunica, pero el análisis de ese servidor intermedio no permite, directamente, que se asocie con NSO Group.

Tanto Citizen Lab como Amnistía Internacional han logrado identificar un buen número de servidores de control de Pegasus en Internet. Sus investigaciones han permitido comprender la "firma" de Pegasus; es decir, determinar un patrón de comportamiento propio de los servidores de control de Pegasus. A partir de ahí, se han podido identificar otros servidores de control de NSO.

De hecho, cada vez que Citizen Lab o Amnistía Internacional publican detalles de cómo son los servidores de control de Pegasus, NSO los modifica, incorporando cada vez más medidas para intentar ocultarlos en Internet. Se han encontrado hasta cuatro versiones de servidores de control de Pegasus, cada una correspondiente a una versión y una época del sistema.

Al final, una monitorización continuada del tráfico que generan dispositivos sospechosos de haber sido infectados con Pegasus puede confirmar su infección, tanto por el volumen de datos generado (si no está justificado por las aplicaciones y el uso del sistema) como por el conjunto de servidores a los que las envía. De hecho, se sabe que el CNI pudo confirmar con este método las infecciones de los móviles de Pedro Sánchez y Margarita Robles.

2.5. Capacidades del sistema Pegasus

Poco se sabe sobre las capacidades concretas del sistema Pegasus, pero se han publicado algunas listas de funcionalidades, que incluyen la grabación de llamadas; la lectura de mensajes de SMS, iMessage y WhatsApp; la lectura de correos electrónicos; el acceso al historial de navegación y a las listas de aplicaciones instaladas; la activación remota del micrófono y de grabación; la activación remota de la cámara, y la retransmisión. No se ha comprobado que incluya el espionaje de la aplicación de mensajería segura Signal, que sí incluye el sistema de ciberespionaje Candiru, competencia de Pegasus y que también se ha utilizado contra políticos catalanes.

Se sabe, asimismo, que Pegasus se puede instalar en terminales iPhone y Android. Candiru también se puede utilizar contra sistemas Microsoft Windows, por lo que se extiende el riesgo de infección a los ordenadores.

Las funcionalidades más mencionadas de los sistemas de ciberespionaje son pasivas, en el sentido de que se limitan a captar información y datos del teléfono y a enviarlos al atacante mediante los servidores C&C intermedios. No obstante, se sabe que algunos de estos sistemas tienen también "funcionalidades activas", con las que el atacante puede enviar correos electrónicos y mensajes suplantando la identidad de la víctima. Se supone que el objetivo principal de estas funcionalidades es la activación de cuentas (banca online, por ejemplo), pero no se descarta que también se puedan utilizar para introducir en los terminales pruebas falsas que puedan incriminar a la víctima en acciones o delitos que no haya cometido.

3. CONTROL DEL SISTEMA DE ESPIONAJE

Un aspecto importante de los sistemas de control informático es la capacidad que tienen para lo que se llama *auditoría*, que no es más que la capacidad de saber quién ha utilizado el sistema, cuándo y por qué.

En sistemas de control legales, como el caso del control informático de equipos o herramientas corporativas, el departamento de informática puede instalar una herramienta de control que pueda monitorizar datos de actividad del personal por alguna razón. Por ejemplo, podría instalarse una herramienta de monitorización de datos de geoposición (por alguna razón legal y autorizada) y, aunque el personal informático pueda tener acceso al sistema para gestionarlo, no debe tener acceso a los datos, puesto que la geoposición es un dato de carácter personal que, en algunos casos, puede ser muy sensible.

Los sistemas informáticos modernos permiten esta "separación de poderes" y en la práctica la dirección de la empresa confía en que el departamento de informática no hará un mal uso de esos datos, y que cumplirá con su deber de información en caso de que alguien (recursos humanos, representación sindical...) pregunte cómo y cuándo se ha utilizado la herramienta, qué datos recoge y quién ha accedido a ella. Las herramientas informáticas modernas pueden tener un registro de actividad no modificable por el propietario del sistema, que puede utilizarse como prueba del uso que se ha realizado.

Cuando se habla de sistemas informáticos que pueden afectar a derechos fundamentales como el derecho a la intimidad o el derecho al secreto de las comunicaciones, la funcionalidad de auditoría debería ser obligatoria. Solo con esta funcionalidad se podrían responder a preguntas como "quién ha sido espiado", "cuánto tiempo ha durado el espionaje" o "qué información ha sido objeto de la monitorización".

Aunque muchos sistemas informáticos actuales, como el correo electrónico, guardan cierta información de actividad, estos datos no están disponibles directamente para los usuarios. Por ejemplo, todos los proveedores de correo guardan una relación de los datos identificativos de las conexiones de Internet que han accedido a las cuentas de correo. Pero estos datos no son ni públicos ni accesibles para la persona propietaria de una cuenta individual (algunos proveedores facilitan datos solo de los últimos días de actividad). Estos proveedores solo facilitan todos los datos mediante un requerimiento judicial, lo que garantiza proporcionalidad y utilidad en el uso de una información que podría ser muy sensible.

En sistemas de ciberespionaje como Pegasus, esta trazabilidad del uso del sistema debería ser una funcionalidad esencial, pero por ahora NSO Group no ha facilitado ninguna información en este sentido sobre Pegasus en los casos que han salido a la luz pública. Es más, existen informaciones contradictorias sobre si realmente NSO puede saber cómo y cuándo sus clientes han utilizado su sistema.

Por una parte, se sabe que NSO Group instala un conjunto de servidores intermedios dedicados a cada cliente por razones de seguridad. Cuesta creer que NSO no monitorice el estado y el uso del sistema

de cada cliente, por ejemplo, para añadir más servidores en caso de que la demanda de servicio de un cliente aumente.

Además, las empresas de ciberespionaje suelen estar sometidas a un importante control de sus gobiernos. Se sabe que NSO Group debe recibir autorización del gobierno israelí para ofrecer sus productos a nuevos clientes, que se limitan a gobiernos, agencias de inteligencia y cuerpos de seguridad de países con intereses comunes.

Este control gubernamental se produce también con otras empresas de ciberespionaje israelíes (Candiru, QuaDream, Paragon) y también en otros países, como Rusia (con Positive Technologies) o China (con Computer Security Initiative Consultancy, que es una empresa de Singapur, pero se cree que opera con tecnología china).

Por último, existe un acuerdo entre Israel y Estados Unidos de no utilizar estos sistemas de ciberespionaje contra ciudadanos estadounidenses. Estas condiciones se han podido ampliar al Reino Unido tras la publicación de que cargos del gobierno de este país podrían haber sido espiados también con Pegasus.

Estas consideraciones hacen difícil creer que Israel no imponga a NSO Group un sistema de trazabilidad de actividad y auditoría sobre el sistema Pegasus, de manera que se pueda saber quién lo utiliza y contra quién. También podría ser que estos datos sean secretos, y también lo sea la existencia misma de los datos.

Por otra parte, los datos publicados denotan una cierta falta de control por parte de NSO Group en el uso que sus clientes hacen de la herramienta. Se han publicado infecciones contra dirigentes políticos de países europeos como Francia, Reino Unido o España, en teoría alineados con los intereses de Estados Unidos (y, por tanto, de Israel). El caso español es interesante, porque ahora se sabe que también es cliente de Pegasus.

Ciertas publicaciones podrían indicar que NSO Group facilita una herramienta a sus clientes que, instalada en un teléfono móvil, informa de si está infectado por Pegasus. Sin embargo, esta herramienta no parece utilizarse en el caso español, donde la detección parece haber sido mediante un análisis de tráfico de datos.

Por otro lado, destaca el uso de Pegasus para una finalidad claramente distinta a las que ha anunciado NSO Group, que, en teoría, son la lucha contra el crimen y contra el terrorismo. Esta finalidad también la han hecho pública otros fabricantes de herramientas de ciberespionaje y, por lo que se sabe, tampoco se ha hecho caso.

Pegasus llamó la atención de grupos como Citizen Lab y Amnistía Internacional precisamente por su uso contra periodistas, políticos y activistas defensores de los derechos humanos. Hay casos documentados desde 2015 en muchos países diferentes, como Arabia Saudí, Marruecos, Emiratos Árabes, Ruanda, Francia, Grecia, Polonia o Hungría.

En España, resulta interesante que el CNI haya admitido que tenía autorización para el ciberespionaje de dieciocho personas del ámbito político catalán, pero que en realidad se hayan documentado más de sesenta casos de espionaje. Aún no se conoce razón alguna que explique esta diferencia, y se duda de que las denuncias iniciadas contra NSO Group acaben con una explicación por parte de la empresa que pueda aclarar la situación.

En definitiva, las funcionalidades de auditoría y trazabilidad de los sistemas de ciberespionaje, tuteladas por los poderes judiciales, son imprescindibles para garantizar un mínimo control del uso de estas herramientas, y esta capacidad de control debería ser transparente, con las evidentes consideraciones de secreto y confidencialidad que también son importantes en estos casos.

4. CAPACIDAD DE DETECCIÓN Y DE DENUNCIA

¿De qué medios técnicos disponemos para detectar *software* de ciberespionaje en nuestros dispositivos? En el caso concreto de Pegasus, sabemos que no se guarda en la memoria interna del teléfono para minimizar la probabilidad de detección, pero las investigaciones de Citizen Lab y

Amnistía Internacional demuestran que, pese a los esfuerzos de NSO Group, la infección y ejecución de Pegasus dejan ciertos indicios y rastros que pueden indicar una posible infección, y permiten saber si un dispositivo ha sido infectado en el pasado.

En concreto, Amnistía Internacional publicó su metodología de análisis completo y la ha ido actualizando con los datos que se han conocido posteriormente. También ha publicado la lista de los indicadores de infección que ha encontrado para el caso Pegasus, y ha puesto a disposición de cualquier usuario de Internet una herramienta gratuita (Mobile Verification Toolkit o MVT) para comprobar la presencia de estos indicadores en su terminal.

La publicación de la metodología es importante, pero permite, evidentemente, que NSO Group tenga la oportunidad de modificar su *software* para evitar que Pegasus, en sus nuevas versiones, deje estos indicios y sea más difícil de detectar. Además, ya han salido también herramientas informáticas que inyectan estos indicadores a móviles para que se provoquen falsos positivos.

Citizen Lab solo ha publicado su metodología parcialmente y ha hecho un análisis de contraste (peer-review) de la metodología de Amnistía Internacional; es decir, mantiene cierta capacidad de rastrear posibles infecciones.

También existen otros métodos de detección. Para empresas grandes o medianas, el análisis de las conexiones realizadas con los teléfonos corporativos y del volumen de datos enviados puede permitir identificar la presencia de sistemas de ciberespionaje no conocidos por los sistemas de antivirus tradicionales. Para empresas y particulares, también existe el recurso de contratar una empresa de peritaje informático o de informática forense.

II. AFECTACIONES A DERECHOS FUNDAMENTALES

1. PREVISIÓN LEGAL EN MATERIA DE INTELIGENCIA

El derecho a la privacidad y al secreto de las comunicaciones está recogido en el artículo 18 de la Constitución Española. Por su parte, el artículo 12 de la Declaración Universal de los Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos reconocen que nadie puede ser objeto de intromisiones arbitrarias en su vida privada, su familia, su domicilio o su correspondencia. Por último, el artículo 8 del Convenio Europeo de Derechos Humanos establece el derecho a la vida privada y familiar, sobre el que solo son aceptables injerencias de las autoridades públicas que estén establecidas por ley, para alcanzar unas finalidades específicas (incluida la seguridad pública y la integridad territorial) necesarias en una sociedad democrática.

Así pues, los derechos fundamentales no son ilimitados y, en determinados supuestos y determinadas condiciones, pueden quedar afectados, siempre respetando su contenido esencial. Estas restricciones y los procedimientos para llevarlas a cabo deben ir acompañadas, tal y como establece la Constitución, de normativa específica en formato de ley orgánica.

Estas injerencias en los derechos fundamentales pueden tener un carácter individual y afectar a un sujeto o un pequeño grupo de sujetos relacionados entre sí, o pueden tener un carácter más general y afectar a los sujetos habituales de un territorio. Entre las primeras, las más frecuentes: las que se derivan de una investigación penal y, en su caso, de las condenas por delitos. Las previsiones desde la detención hasta el encarcelamiento de personas, pasando por limitaciones en los derechos que afecten a la intimidad en sus diversas vertientes o a la propiedad, están previstas en las leyes procesales. La extralimitación en la puesta en práctica de estas lesiones, en principio legítimas, son sancionadas también por ley, ya sea declarando la nulidad de las medidas adoptadas o exigiendo responsabilidades personales a quien las haya adoptado o ejecutado.

En este sentido, las medidas que se adoptan por mandato o autorización expresa de la Constitución son bien de carácter investigador –como las diligencias penales, en las que se analizan unos hechos porque existen indicios de la comisión de un delito– o bien de carácter defensivo o preventivo, frente a determinados peligros establecidos en la propia Constitución, como por ejemplo el estado de alarma en diversas intensidades que se ha vivido recientemente a causa de la covid, o los estados de excepción o de confinamiento.

En defensa del Estado se pueden utilizar un gran número de medidas, entendidas en sentido amplio y más allá de los conceptos tradicionales y legales de la seguridad nacional. Ante determinados indicios, la ley prevé que una institución concreta y específica que depende del Gobierno y sigue sus directrices anuales, el CNI, pueda poner en marcha investigaciones tanto de sujetos aislados como, más frecuentemente, de grupos de ciudadanos, españoles o extranjeros, que puedan afectar al ordenamiento constitucional vigente.

Para llevar a cabo estas funciones de inteligencia (es decir, una investigación para obtener información y la interpretación de esa información para darle sentido), de acuerdo con las previsiones legales, puede ser necesario, por un lado, llevar a cabo registros en lugares cerrados, tales como domicilios o despachos, y por otro, comprobar ciertas comunicaciones. Las funciones que de forma más o menos difusa encomienda la ley al CNI (Ley 11/2002, art. 4), conllevan unas necesidades de injerencia en los derechos que integran la intimidad personal, familiar y profesional.

La cobertura constitucional de estas intervenciones se encuentra en el enunciado genérico del artículo 18.3 de la Constitución, que las somete a autorización judicial: “Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial”.

Amparada en esta habilitación, la Ley reguladora del control judicial previo del CNI prevé que este organismo solicite a un magistrado del Tribunal Supremo la “intervención de las comunicaciones” (Ley orgánica 2/2002, artículo único). La ley no especifica que esta actuación deba ser

motivada y, además, puede ser reiterada sin límite. Los resultados de las investigaciones no deben comunicarse al magistrado que las autorizó, y ni siquiera la petición ni la resolución deben formularse por escrito. Eso sí, en ningún caso los resultados de este tipo de investigaciones pueden integrarse en un proceso penal, dado que responden a una mecánica distinta a la del proceso penal, tanto material como formalmente, es decir, en contenido y garantías.

2. DIFERENCIAS ENTRE INVESTIGACIÓN PENAL E INVESTIGACIÓN DE INTELIGENCIA

La investigación penal se pone en marcha porque existen indicios razonables de la comisión de un hecho con carácter delictivo. Por el contrario, las investigaciones de inteligencia se llevan a cabo para observar qué ocurre en ámbitos no fácilmente accesibles, más bien clandestinos o, al menos, alejados del escrutinio y la observación públicos, pero sensibles a los objetivos funcionales del CNI, sin que estos asuntos deban tener ni siquiera indiciariamente carácter de delito. Por ello, a diferencia de las investigaciones penales, las de inteligencia constituyen investigaciones prospectivas, una modalidad prohibida constitucionalmente en las investigaciones penales, y son más proclives, por tanto, a la invasión de esferas de intimidad de forma no siempre legítima.

El bien que se protege en una investigación penal es el que integra el objeto de protección de cada definición legal de delito; es decir, la vida, la libertad, la integridad sexual, la intimidad... En cambio, los objetivos que definen las actividades de inteligencia no están estrictamente definidos en la Constitución y los que sí se definen lo están con un grado de indeterminación que permite un amplísimo radio de acción, con fácil peligro de desbordamiento.

En este punto cabe comparar los requisitos que deben seguir las órdenes judiciales que afecten a derechos fundamentales en procesos penales o actuaciones de inteligencia. La regulación del proceso penal en materia de investigaciones que afecten a los derechos que integran la intimidad de los ciudadanos está estrictamente regulado, especialmente después de 2015. Por regla general, la inobservancia de los requisitos legales comporta, como mínimo, la nulidad de las pruebas que hayan podido obtenerse mediante estas injerencias defectuosas. En cambio, no se observa previsión legal alguna que permita expulsar del ordenamiento jurídico actuaciones de inteligencia que no cumplan ni los requisitos mínimos previstos en la ley del sector.

Ahora bien, centrados en el tema que motiva este informe, el llamado Catalan Gate, dado que no ha trascendido el contenido de ninguna petición de autorización por parte del CNI, en principio no se puede valorar si la petición administrativa ha cumplido, aunque de forma aproximada, los parámetros que deben revestir tanto las peticiones policiales en sede de investigación criminal como los autos judiciales que las autorizan. Esta doctrina y su base legal podrían dar cierta entidad a la simple regulación prevista por la actuación gubernativa de inteligencia, tanto en lo que se refiere a la formulación de la petición de la autorización judicial como al otorgamiento de la autorización.

Cabe decir, ciertamente, que el Defensor del Pueblo, tras analizar los autos del Tribunal Supremo que autorizaban las intervenciones en los dispositivos móviles de las dieciocho personas objeto de supervisión en el caso Catalan Gate, ha constatado el "elevado grado de detalle en la información de que disponía el magistrado del Tribunal Supremo para poder adoptar una decisión de autorización o no autorización" y que los autos "estaban extensamente motivados, esencialmente fundados en hechos concretos".

Sin embargo, teniendo en cuenta los derechos sobre los que versa la petición de autorización por parte de los servicios de inteligencia, y en vista de las informaciones hechas públicas por Citizen Lab, que nadie ha contradicho, el Síndic plantea, como mínimo, una serie de dudas sobre los posibles derechos fundamentales afectados, y concluye con unas recomendaciones derivadas de la doctrina del máximo órgano protector de los derechos fundamentales en Europa: el Tribunal Europeo de Derechos Humanos (TEDH).

Con los datos disponibles, y dado el secreto legal que protege las actuaciones practicadas (tanto las dieciocho que se han reconocido públicamente como las otras), puede

concluirse que toda injerencia en los derechos fundamentales previstos por la Constitución se construye sobre dos pilares esenciales. Uno es la necesidad y el otro, la proporcionalidad. El presupuesto de ambos pilares es el principio de legalidad.

A continuación, se analizan estos elementos en relación con los derechos que, presumiblemente, han sido o han podido estar afectados por las injerencias mencionadas.

3. PRINCIPIOS RECTORES DE LAS INJERENCIAS EN MATERIA DE DERECHOS FUNDAMENTALES (I): EL PRINCIPIO DE LEGALIDAD

Empecemos por la base común de todas las afectaciones provocadas por los poderes públicos que quieren ser justificadas en la esfera de los derechos de los ciudadanos. La condición o el requisito de legalidad opera en una doble vertiente. La primera resulta obvia: la medida que debe practicarse en la esfera de los derechos básicos debe venir específicamente prevista por la ley; en este caso, la ley debe ser la propia Constitución, desarrollada por ley orgánica. En cuanto a lo que nos ocupa, la ley prevé que es necesaria autorización judicial para acceder a las comunicaciones de los sujetos que se quiere monitorizar.

3.1. El principio de legalidad: ámbito de la injerencia

Tal y como se ha visto en la primera parte de este informe, dado que la injerencia llevada a cabo por la tecnología Pegasus supone un acceso íntegro a los teléfonos móviles, cabe subrayar que, con la ley en la mano, es ilegal acceder al conjunto de información y a los datos que incorpora el teléfono móvil infectado. En efecto, según la Constitución, solo es lícito acceder a las comunicaciones, es decir, a contactos interpersonales mediante el sistema de redes físicas o virtuales de que se dispone. No es lícito, en cambio, acceder al resto de información que puede contener un dispositivo de ese tipo, que es mucha.

Este extremo es de vital importancia si tenemos en cuenta que, como se ha visto, los *smartphones* son mucho más que teléfonos convencionales; son, de hecho, ordenadores miniaturizados, multifuncionales, con infinidad de datos que nada tienen que ver con comunicaciones interpersonales. Por ejemplo, la agenda diaria, los contactos, los archivos documentales, gráficos, sonoros o de imágenes en cualquier formato (incluso películas de todo tipo), los datos escaneados, los códigos QR o las fotos familiares que se llevan en los teléfonos no son comunicaciones, sino objetos que pertenecen a la persona titular del teléfono, independientemente de la forma en que las fotos, los datos o los otros documentos se hayan introducido en el aparato.

Es más, el acceso a documentos u otros archivos que se encuentran en la nube y que pueden ser descargados en los teléfonos no constituye propiamente una comunicación, dado que no se establece una comunicación interpersonal. En efecto, la comunicación no se hace con otra persona distinta a la titular, sino que configura el acceso en remoto a un archivo propio que se puede descargar en su totalidad o en parte, o incluso simplemente se puede visualizar, sin contactar con nadie más.

Igualmente resulta de interés que, a diferencia de lo que sucede con materia de investigación criminal legítimamente autorizada, el seguimiento de personas mediante el teléfono es ajeno al concepto legal de comunicación, dado que la deambulación, el traslado o el transporte de una persona físicamente no implica ninguna intercomunicación personal. Seguir una baliza instalada en un teléfono móvil no es comunicación entre dos sujetos, uno de los cuales es objeto de la investigación.

Así, con la legislación española en mano, y sin necesidad de verificar el contenido de ninguna petición ni de ninguna autorización judicial, resulta legítimo afirmar que en ningún caso se puede acceder legalmente a un teléfono, en una investigación de inteligencia, para obtener información diferente de las comunicaciones interpersonales.

3.2. El principio de legalidad: las razones de la injerencia

Una segunda vertiente de la legalidad referida al campo de la inteligencia tiene relación con los motivos o razones que

afectan a la integridad del llamado *sistema institucional vigente*. Ciertamente, se trata de un concepto vaporoso y poco definido y definible. Ahora bien, nada tienen que ver con la integridad del sistema institucional las actuaciones de inteligencia dirigidas hacia las comunicaciones interpersonales cuando se refieren a situaciones que afectan a otros derechos fundamentales diversos de la intimidad, o a objetivos ajenos a esta institucionalidad básica, como pueden ser intereses políticos, personales o comerciales.

De este modo, estas actuaciones quedan huérfanas de cobertura legal y, por tanto, el principio de legalidad queda vulnerado en este sentido cuando, como se ha sabido, se observan comunicaciones y más elementos integrantes de la intimidad de las personas y que afectan a otros derechos fundamentales, como es el derecho de defensa o las negociaciones entre partidos para formar gobierno tras unos comicios.

a) El derecho de defensa

El derecho de defensa no solo integra la defensa de las pretensiones de las personas interesadas frente a los tribunales y otros poderes públicos, sino que se basa en la confidencialidad que preside sin excepciones las relaciones entre abogado y cliente. En el caso más extremo, el de las imputaciones de los delitos más graves –en los que, por tanto, ya existe una causa constituida procesalmente–, el derecho a la defensa y libertad de las comunicaciones entre el letrado y su cliente es inalienable en cualquier lugar y cualquier circunstancia.

Hay derechos, como la libertad personal o el secreto de las comunicaciones, que pueden ser suspendidos individual o colectivamente. No es el caso de la confidencialidad entre abogado y cliente, que, como decíamos, constituye la base del derecho de defensa y, a su vez, una de las manifestaciones del derecho a un proceso público con todas las garantías. Este derecho no puede sufrir restricción alguna en ninguna circunstancia. Tanto es así que la vulneración de este derecho ha supuesto alguna sanción penal grave, incluso contra algún juez, y ha redundado en la inhabilitación para el ejercicio de funciones públicas de los responsables.

En el contexto de las autorizaciones judiciales prospectivas puede producirse una situación crítica que, de hecho, podría dejar inoperativo el derecho a la defensa y a la confidencialidad entre abogado y cliente. Puesto que los magistrados que pueden dar estas autorizaciones pertenecen a dos salas en las que algunas de las personas investigadas tienen pleitos pendientes –es decir, las salas contencioso-administrativa y penal, ambas del Tribunal Supremo–, estos magistrados, al autorizar la observación de las comunicaciones de estas personas podrían entrar en contacto y en secreto con sus estrategias procesales. Esto comportaría una lesión irreparable del derecho de defensa.

Tal y como se indica más adelante, cabe añadir que, dado que la designación de estos magistrados no se hace según un sistema público y objetivo, sino según un sistema dirigido a la elección de un juez determinado por razones que no constan en la ley, la sombra de duda sobre el derecho de defensa se hace aún mayor y se acerca más a la línea de un riesgo constitucionalmente inasumible.

b) El derecho a la participación política

El derecho de participación en asuntos públicos tampoco es susceptible de afectación legítima, en ningún contexto. Acceder a las comunicaciones y otros contactos, interceptar documentos u observar negociaciones, sean formales o meros contactos entre formaciones políticas, es radicalmente contrario a la legislación vigente. La confidencialidad que preside estas negociaciones es la que las partes quieran darle y, por tanto, corresponde solo a las fuerzas en trámite de negociación revelar al público lo que van acordando o el estado general de las negociaciones. Infringir este derecho es aún más grave, dado que se vulneran los derechos de los representantes y de sus representantes. En efecto, se trata de negociaciones entre fuerzas políticas sobre las que no existe presunción alguna de ilegalidad, persigan las finalidades que persigan, ya que la Constitución Española no es, a diferencia de otras, una constitución militante. El derecho a la participación en los asuntos públicos ha quedado, en este caso, comprometido.

3.3. El principio de legalidad: el juez predeterminado por la ley

El juez designado para autorizar las injerencias en las comunicaciones de los ciudadanos es designado *ad hoc*, sin concurso, por el Pleno del Consejo General del Poder Judicial (art. 127.4 de la Ley orgánica 6/1985, de 1 de julio, del poder judicial).

La Constitución establece como derecho fundamental básico de la persona, como un derecho fundamental que garantiza la imparcialidad objetiva judicial y la seguridad jurídica, que los jueces vengan determinados por la ley, a todos los efectos y no para un asunto concreto. Con esta designación personal de un juez para un asunto concreto y tan sumamente delicado, se corre el riesgo de que la competencia sobre este asunto no venga predominada por un turno legal, como sucede en el resto de los asuntos litigiosos, sino que se busque un juez para un tipo de caso concreto y único con unas características específicas. En este supuesto, no es la ley sino estas características de orden personal lo que establecería la competencia. Esta forma de designación personal puede vulnerar el carácter de previsión generalista de asignación de competencias, tal y como prevé el ordenamiento vigente para el conocimiento de los asuntos jurisdiccionales.

La regulación actual, en cierta medida de dudosa constitucionalidad, parece más bien idónea para designar a un magistrado a priori más favorable a las pretensiones del CNI que a la salvaguarda de los derechos de los ciudadanos.

4. PRINCIPIOS RECTORES DE LAS INJERENCIAS EN MATERIA DE DERECHOS FUNDAMENTALES (II): EL PRINCIPIO DE NECESIDAD

En cuanto a la necesidad, es bien sabido que, tal y como ha señalado la jurisprudencia, tanto ordinaria como constitucional, la afectación de derechos fundamentales debe ser realmente el último recurso, es decir, si no hay otra medida posible que responda a los objetivos de los investigadores. Del mismo modo, también como apunta la jurisprudencia, no puede confundirse la comodidad del órgano o la facilidad en la ejecución de la medida con la necesidad de esta medida.

La necesidad de la injerencia supone realmente el último medio de que dispone el poder público correspondiente. Dicho de otro modo, si se dispone de formas que, aunque sean más dificultosas, sean menos invasivas, deben emplearse. Por este motivo, solo es constitucionalmente legítima la ejecución de estas medidas invasivas de derechos fundamentales en la medida en que no sea factible otra forma de actuar.

Ahora bien, en estos momentos no existe ningún elemento exterior y accesible que permita valorar este extremo para formular las peticiones y emitir la resolución judicial que las autorice, incluso condicionando su práctica al requisito de la necesidad.

Además, este requisito viene impuesto por la autorización de la intervención y, en su caso, por la autorización de la prolongación. Dicho esto, cabe resaltar que no existe previsión legal alguna respecto a la ponderación judicial del resultado final. Esto tiene como consecuencia que, en definitiva, la necesidad de la injerencia en las comunicaciones pueda convertirse en una apreciación meramente proforma y nunca verificada materialmente por una autoridad independiente.

Finalmente, cabe reiterar que, desde el punto de vista de la previsión legal, solo puede ser masiva la observación de las comunicaciones y no de otros objetos que se puedan obtener debido a que se encuentran en el dispositivo móvil o en cualquier otro tipo de dispositivo que permita comunicaciones interpersonales, tanto si el alcance de la observación es sobre un sujeto como sobre un grupo de sujetos.

5. PRINCIPIOS RECTORES DE LAS INJERENCIAS EN MATERIA DE DERECHOS FUNDAMENTALES (III): EL MANDATO DE PROPORCIONALIDAD

En este terreno, la proporcionalidad o, en términos negativos, la prohibición del exceso, desempeña un papel preponderante en el terreno de las injerencias en los derechos fundamentales. A la hora de interceptar las comunicaciones llevadas a cabo desde un teléfono móvil –como los

teléfonos inteligentes actuales– o desde otros dispositivos –como los ordenadores de sobremesa, ordenadores portátiles y todo tipo de tabletas conectados a la red de telecomunicaciones–, no se puede acceder a otros objetos que no sean las propias comunicaciones. Cabe recordar que quedan constitucional y legalmente excluidos todo el resto de los materiales que se encuentren, con independencia del interés por obtenerlos y analizarlos. Así, el mandato de proporcionalidad impone la destrucción inmediata, sin más contacto que esa destrucción, de los datos que se obtengan en un aparato susceptible de observación.

Dicho esto, y siguiendo las pautas elaboradas por la Comisión de Venecia de 2015[3] en relación con las observaciones de inteligencia y un conjunto de sentencias del TEDH,[4] se ha ido configurando una doctrina sólida en la que la necesidad y la proporcionalidad son la base de las funciones de inteligencia sobre las comunicaciones y otros aspectos de la intimidad.

Ya no se trata solo de la concepción clásica de la proporcionalidad como un juicio sobre el hecho de que los beneficios de la injerencia en los derechos fundamentales deben superar la inevitable lesión de estos. Se trata, además, de que estos juicios de necesidad y proporcionalidad deben ser verificados con posterioridad, al menos una vez llevada a cabo la observación, y debe valorarse en qué medida los derechos a la intimidad y los demás derechos fundamentales se han visto afectados según los parámetros constitucionales.

Esta verificación debe tener en cuenta, como mínimo, tres factores fundamentales. En primer lugar, la verificación del proceso de injerencia debe llevarlo a cabo un ente independiente, ajeno al ente que lleva a cabo la investigación de inteligencia, que puede ser judicial o no. En segundo término, deben verificarse de forma independiente los resultados obtenidos con las injerencias en los derechos fundamentales vulnerados. Por último, es necesario dar la oportunidad a la persona afectada de verificar la afectación y poder recurrir a los tribunales, llegado el caso, si observa que se han vulnerado sus derechos constitucionales.

Ninguno de los organismos mencionados, ni la Comisión de Venecia ni el TEDH, niegan la necesidad de las investigaciones de inteligencia, incluso masivas, en las áreas más sensibles de la sociedad actual. Estas injerencias, sin embargo, deben llevarse a cabo con las garantías esenciales en una sociedad democrática. Al fin y al cabo, el control de la legitimidad de la injerencia, que solo puede llevarse a cabo con posterioridad, debe poder hacerlo tanto un órgano independiente como la persona afectada. Es lo que el TEDH denomina en sus resoluciones *end-to-end safeguards*; es decir, poder someter las injerencias en los derechos fundamentales a un control de principio a fin, de modo que el proceso de injerencia cumpla todas las garantías. De hecho, esto es lo que sucede en los procedimientos o en aplicaciones digitales complejos, en las que las verificaciones de los procedimientos son automáticas, sin necesidad de añadir ningún elemento más.

El disfrute efectivo de estas garantías solo es posible si las personas afectadas son conocedoras, en un momento dado, de la intromisión de la que han sido objeto. Por este motivo, el informe de Amnistía Internacional de mayo de 2022 no solo afirma que es imprescindible la supervisión judicial, sino que las personas afectadas deben ser informadas, cuando sea posible, de que han sido objeto de medidas de vigilancia o de que sus datos han quedado comprometidos.

[3] Comisión de Venecia. *Report on the Democratic Oversight of Signals Intelligence Agencies*, aprobado en la 102ª sesión plenaria (Venecia, 20-21 de marzo de 2015). Estudio núm. 719/2013, Estrasburgo, 15 de diciembre de 2015.

[4] Véanse las sentencias de la Gran Sala del TEDH de 4 de diciembre de 2015 (caso Roman Zakharov *vs*. Rusia) y de 25 de mayo de 2021 (casos Big Brother Watch *vs*. el Reino Unido y Centrum för Rättvisa *vs*. Suecia.

III. CONCLUSIONES

Los sistemas de ciberespionaje global son una realidad en Europa y provocarán un debate y una reflexión sobre la forma en que las agencias de inteligencia y los cuerpos de seguridad deben controlar el uso de estos recursos tecnológicos.

Sin duda los gobiernos y las agencias de inteligencia necesitarán de estos servicios, ya sean propios, como es el caso de países con recursos tecnológicos como Estados Unidos, Rusia o China, o contratados, como en la mayoría de los países europeos. También deberán aprender a defenderse y evitar situaciones como las ocasionadas por Pegasus en España, Reino Unido, Francia o Grecia.

A juzgar por la información disponible se puede presumir que el uso de estos sistemas sobre los dieciocho ciudadanos mencionados ha respetado la legalidad formal, pero al mismo tiempo es indudable que puede haber supuesto un atentado a sus derechos fundamentales, incluido el derecho a la privacidad y, en algunos casos, a su derecho de defensa y participación política. Para el resto de las personas presuntamente espiadas con Pegasus, más de cuarenta, todo apunta a que no se ha respetado ningún tipo de legalidad y que la injerencia sobre sus derechos fundamentales ha sido sin restricciones y sin control alguno.

Por este motivo, desde el punto de vista de la salvaguarda de los derechos humanos y de las libertades fundamentales, el Síndic de Greuges considera lo siguiente:

1. Según el examen obligado de las actuaciones que ha reconocido el CNI y de las que han documentado Citizen Lab y Amnistía Internacional y que no se han contradicho, se puede presumir que se han producido lesiones injustificadas en los derechos de las personas observadas, en aspectos de su intimidad personal, familiar y profesional, en su derecho de defensa, en su derecho a la confidencialidad entre cliente y abogado, en su derecho a participar en la gestión de los asuntos públicos por sí mismos o por medio de sus representantes y en su derecho a un juez predeterminado por la ley. Por tanto, debería producirse una reparación por parte de los poderes públicos implicados.

2. La intervención en las "comunicaciones", prevista constitucional y legalmente como límite del derecho a la intimidad, no ampara en ningún caso, ni siquiera con autorización judicial, el acceso a toda la información que puede haber en los terminales móviles de tipo teléfono inteligente.

3. Es necesaria una reforma urgente de la ley de secretos oficiales, que se acomode a las reglas emanadas de la Comisión de Venecia y del TEDH. En este sentido, es necesario establecer un sistema público y colegiado de autorización y control judiciales respecto de las observaciones de las comunicaciones que en sede de inteligencia se soliciten en el marco de la ley. En efecto, por un lado, debe pasarse de un sistema de juez individual a tribunal colegiado y, por otro, la designación de sus integrantes debería ser pública, en todo caso, mediante el correspondiente concurso entre los magistrados del Tribunal Supremo, si se estima conveniente. El nombramiento del magistrado encargado de las autorizaciones y los controles no podrá depender del designio único del presidente del Consejo General del Poder Judicial, ratificado proforma por el pleno del Consejo.

4. Es necesario, además, fijar un límite temporal a las observaciones de las comunicaciones, dado que con el diseño legal actual podrían ser indefinidas, sin que el sujeto observado hubiera cometido infracción alguna del ordenamiento jurídico ni tuviera conocimiento de que está siendo monitorizado.

5. Una vez finalizada la actuación gubernativa de observación y concluida con una resolución judicial valorativa, habría que informar a la persona interesada, de forma reservada, pero con pleno acceso al expediente administrativo y judicial generado, a fin de que pudiera alegar lo que considere oportuno sobre la posible vulneración de sus derechos. De esta forma, la persona recibiría una resolución fundada jurídicamente y recurrible, si cabe, en salvaguarda de sus garantías constitucionales.

6. La ley debe expresar explícitamente que quedan excluidas de investigación las observaciones de miembros de partidos

políticos, sindicatos y asociaciones de cualquier tipo que sean legales, es decir, constituidos conforme a las leyes y sin estar sancionados, lo que incluye la disolución judicial o, incluso, la prohibición.

7. Debe quedar también establecida en la letra de la ley la prohibición de observar las relaciones entre cliente y abogado o de interferir en ellas de cualquier modo. Estas relaciones no pueden ser objeto de observación o registro en ningún caso y en ninguna circunstancia. En estos dos últimos supuestos, la reforma de ley debería hacer especial referencia a la responsabilidad penal si se producen dichas anomalías. Desde este punto de vista, el Síndic recomienda a los colegios profesionales de la abogacía de Cataluña, y al consejo de colegios en particular, que promuevan acciones de garantía del derecho de defensa en los casos en que las relaciones entre cliente y letrado se hayan visto afectadas por escuchas ilegales.

8. Los fabricantes de los sistemas de ciberinteligencia deberían estar sometidos a controles de auditoría y estar obligados a identificar a clientes y víctimas en ciertas condiciones compatibles con el secreto que su actividad requiere. Tecnológicamente hablando, esa trazabilidad es posible y compatible con el respeto a la confidencialidad de las personas implicadas. Las funcionalidades de auditoría y trazabilidad de los sistemas de ciberespionaje, tuteladas por los poderes judiciales, son imprescindibles para garantizar un control mínimo del uso de estas herramientas, y esta capacidad de control debería ser transparente, con las evidentes consideraciones de secreto y confidencialidad que también son importantes en estos 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