AL JUZGADO DE INSTRUCCIÓN DE MADRID QUE POR TURNO CORRESPONDA

D. Procurador Carlos Ricardo ESTÉVEZ SANZ de los Tribunales de Madrid, según acredito mediante firma original de la presente querella por parte de mi representado[1], ante el Juzgado comparezco y como mejor proceda en Derecho, **DIGO:**

Que, por medio del presente escrito, vengo, en la representación que ostento, a interponer **QUERELLA**, de conformidad con lo establecido en el artículo 277 de la Ley de Enjuiciamiento Criminal y en el ejercicio de la **ACUSACIÓN PARTICULAR**, al amparo de lo establecido en el artículo 24.1 de la Constitución Española, y en los artículos 101 y 277 de la Ley de Enjuiciamiento Criminal, por la presunta comisión de los delitos previstos y penados por los arts. 197.1, 197 bis.1 y 197 quater, así como cualquier otro delito que aparezca en el transcurso de la investigación de los hechos que se denuncian contra "Q CYBER TECHNOLOGIES L.T.D.", y sus subsidiarias "N.S.O. GROUP TECHNOLOGIES L.T.D." en Israel y "OSY TECHNOLOGIES S.à.r.l." en Luxemburgo, así como también contra Niv KARMI, Shalev HULIO, Omri LAVIE y cuantas personas más

[1] *En caso de considerarse necesario, y a pesar de venir la presente querella firmada por abogado, procurador y el propio querellado, se le requiera a través de la presente representación para que la ratifique apud acta o aporte un poder especial para querella.*

resulten responsables en los hechos objeto de la presente querella.

I – JUZGADO ANTE EL QUE SE PRESENTA

Esta querella se presenta ante el Juzgado de Instrucción de Madrid que por turno corresponda por ser competente con arreglo a los artículos 14, 272 y concordantes de la Ley de Enjuiciamiento Criminal al haberse cometido en ese partido judicial los hechos que se relacionan en este escrito.

II – NOMBRE Y DOMICILIO DEL QUERELLANTE

El querellante en el ejercicio de la acusación particular es D. Gonzalo BOYE, con domicilio a efectos de notificaciones en la Calle Pilar de Zaragoza, 9 - 28028, Madrid.

III – NOMBRE Y DOMICILIO DE LOS QUERELLADOS

1. "Q CYBER TECHNOLOGIES L.T.D.", con domicilio declarado en Galgalei Haplada, 22, Herzliya, 4672222, Israel.

2. “N.S.O. GROUP" TECHNOLOGIES L.T.D.”, con domicilio declarado en Galgalei Haplada, 22, Herzliya, 4672222, Israel.
3. “OSY TECHNOLOGIES S.à.r.l.”, con domicilio declarado en Rue Edward Steichen, 2, Luxemburgo, código postal 2540.
4. D. Niv KARMI, con domicilio a efectos de notificaciones en Galgalei Haplada, 22, Herzliya, 4672222, Israel.
5. D. Shalev HULIO, con domicilio a efectos de notificaciones en Galgalei Haplada, 22, Herzliya, 4672222, Israel.
6. D. Omri LAVIE, con domicilio a efectos de notificaciones en Galgalei Haplada, 22, Herzliya, 4672222, Israel.

Así como todos aquellos otros que resulten responsables de los hechos de la presente querella a lo largo de la investigación.

IV – RELACIÓN CIRCUNSTANCIADA DE LOS HECHOS

IV.I.- INTRODUCCIÓN

De acuerdo a lo que se establecerá en el presente escrito, se infiere la ilegalidad del software de inteligencia cibernética “Pegasus”, creado y administrado por “N.S.O. GROUP

TECHNOLOGIES L.T.D.”, su indebido uso tanto en España como en otros países, y en el caso concreto que nos ocupa, su utilización para la comisión de hechos delictivos que, indiciariamente y sin perjuicio del análisis que deberá efectuarse durante el transcurso de la investigación.

IV.II.- CONTEXTO

Previo a exponer la relación circunstanciada de los hechos delictivos que son objeto de la presente querella, corresponde efectuar algunas consideraciones acerca del software de inteligencia cibernética “Pegasus”, así como también acerca de la compañía creadora y administradora de aquél, “N.S.O. GROUP TECHNOLOGIES L.T.D.” y sin cuya participación necesaria nada de lo sucedido habría sido posible, de la indebida utilización de este software espía en diferentes países y del contexto político en Catalunya, el que, como se verá, se encuentra íntimamente vinculado con la comisión de los hechos delictivos a los que se hará mención más adelante.

IV.II.A.- SOBRE "PEGASUS"

El programa espía "Pegasus" es un software malicioso de inteligencia cibernética que permite extraer, de forma remota y secreta, información ilimitada desde prácticamente cualquier dispositivo móvil[2], y a su vez, recopilar, clasificar y transmitir de un modo efectivo e integral los datos recogidos del dispositivo móvil para su ilegal análisis[3]. Desde el año 2012 fue catalogado oficialmente por el estado de Israel como un **arma de inteligencia cibernética**, y si bien dicho estado autorizó su comercialización, condicionó aquélla a que se realice exclusivamente con autoridades públicas o agencias estatales a las que autorice expresamente el Ministerio de Defensa de ese país.[4]

"Pegasus" tiene la capacidad de penetrar los dispositivos basados en Android, BlackBerry, iOS, Symbian y Windows, así como también los dispositivos protegidos con contraseña[5].

La instalación del software de que se trata (denominado "agente") se realiza de forma remota (tecnología "over-the-air"), no requiere, en la actualidad, ninguna acción ni interacción

---

[2] *Brochure "Pegasus", pág. 1.*
[3] *Brochure "Pegasus", pág. 2.*
[4] *Qué es "Pegasus": así funciona el software de espía israelí que hackea a medio mundo.*
[5] *Brochure "Pegasus", pág. 3.*

con el objetivo y no deja rastro en el dispositivo atacado[6]. En caso de que por alguna razón no pueda instalarse de forma remota, el "agente" también tiene la capacidad de ser instalado mediante un mensaje de texto (SMS) con un enlace "malicioso" ("malware"), el cual una vez aceptado por el objetivo despliega automáticamente la instalación del software[7].

Una vez instalado remota y secretamente en el dispositivo móvil, el "agente" puede acceder de forma ilimitada al dispositivo actuando como si de una réplica de dicho dispositivo se tratase. Entre algunas de sus funcionalidades y características, se pueden destacar:

- Interceptación de las llamadas entrantes y salientes del dispositivo (monitoreo de llamadas de voz y VoIP[8] en tiempo real);
- Recopilación de información de contactos, de archivos, de imágenes, de videos, de escuchas telefónicas ambientales, de registro de llamadas entrantes y salientes, de historial de navegación web, de contraseñas, de mensajes de texto (SMS), de mensajería

[6] *Brochure "Pegasus", pág. 3.*
[7] *Qué es "Pegasus": así funciona el software de espía israelí que hackea a medio mundo.*
[8] *Denominado por sus siglas en inglés "Voice over the internet protocol", es una tecnología que permite ejecutar comunicaciones de voz o sesiones multimedia (tales como de video) a través de internet.*

instantánea, de correos electrónicos, de registros de calendario, etc;

- Captura de imágenes -fotográficas y de vídeo- desde la cámara del dispositivo y capturas de pantalla;
- Activación y grabación de voz desde el micrófono del mismo;
- Monitoreo de aplicaciones como Skype, Whatsapp, Viber, Facebook y Mensajero de BlackBerry (BBM);
- Localización de objetivos (seguimiento de objetivos y obtención de información sobre la posición exacta con GPS);
- Independencia del proveedor de servicios (no necesita la cooperación con los operadores de redes móviles -MNO[9]-);
- Monitoreo del dispositivo sin tener que preocuparse por el cambio frecuente de identidades virtuales y el reemplazo de tarjetas SIM[10].

La recopilación de datos que realiza "Pegasus" es, como se dijo, prácticamente ilimitada, y de acuerdo a lo que detalla "N.S.O. GROUP", se divide en 3 niveles:

1) Extracción de información inicial: una vez que el agente se encuentra correctamente instalado en el dispositivo

[9] *Por su siglas en inglés significa "Mobile Network Operator", referido a Operadores de Redes Móviles.*
[10] *Brochure "Pegasus", pág. 3 y Complaint NSO.pdf, pág. 40.*

móvil el software extrae y transmite el historial de mensajes (SMS), el detalle de contactos, el historial de llamadas entrantes y salientes, los registros de calendario, los correos electrónicos, los registros de mensajería instantánea y el historial de navegación web, entre otros datos;

2) Monitoreo pasivo: luego de extraer toda la información que se detalló precedentemente, este software también tiene la capacidad de continuar monitoreando aquélla y extraer toda nueva información que se reciba o se transmita en tiempo real, así como también realizar un monitoreo del dispositivo basado en "Cell-ID[11]".

3) Recopilación activa: además del monitoreo pasivo, el agente tiene la capacidad de recopilar información específica a través del mismo software en tiempo real a solicitud del interesado. A saber, y cuando se lo requiera, el agente puede hacer un seguimiento de la posición del objetivo vía GPS, interceptar las llamadas telefónicas, recuperar archivos, ejecutar grabaciones de sonido ambiental

[11] *Traducido del inglés, se refiere a "Identificador de Celda", que es el número único de la torre GSM (sistema global de comunicaciones) a la que el dispositivo móvil de que se trate está conectado en ese momento.*

a través del micrófono del dispositivo, capturar imágenes a través de la cámara del dispositivo, tomar capturas de pantalla, etc.[12]

Además de tener la capacidad de extraer de forma remota y secreta la información del dispositivo móvil y transmitir esa información para su análisis, este software de inteligencia cibernética tiene herramientas para filtrar y ordenar los datos recogidos en base a consultas y búsquedas de texto libre, para enviar alertas tras la llegada de datos importantes y para marcar los eventos importantes y favoritos[13], así como para alterar, introducir y extraer documentos del dispositivo atacado.

Si bien "N.S.O. GROUP" presenta y describe la arquitectura del software "Pegasus" de un modo extremadamente pormenorizado, al que se hizo referencia ut supra lo cierto es que, llamativamente, ello no es así con respecto a la política de protección de la ilimitada cantidad de datos que pueden ser recopilados -la gran mayoría de ellos extremadamente sensibles desde una perspectiva del derecho al secreto de las comunicaciones y del derecho a la intimidad- que, en el presente caso, el del Letrado Sr. Boye,

[12] *Complaint NSO.pdf, págs. 41/42.*
[13] *Brochure "Pegasus", pág. 3.*

afecta también al secreto profesional y al derecho de defensa de sus clientes.

No se especifica en qué servidores es alojada la información, ni por quién es administrada, ni por cuánto tiempo es conservada y, ni mucho menos, si luego de su utilización es destruida o no, aunque por algunas informaciones aparecidas en medios israelíes, a raíz de un reciente escándalo de espionaje en dicho país mediante el uso del mismo sistema, **podemos asumir que esos datos se almacenan en los propios servidores de "N.S.O. GROUP" y desde ahí son administrados y remitidos, total o parcialmente, a sus clientes que son, en definitiva, quienes hacen uso de los mismos**[14] sin que se descarte, en estos momentos, que **los propios querellados pueden hacer uso de esos datos o cederlos y/o venderlos a terceros.**

Esta cuestión resulta el foco central que sustenta la ilegalidad de este software de inteligencia cibernética, pues, como se desarrollará más adelante, aún cuando su utilización se lleve a cabo en el marco de una investigación judicial -que no es el caso- por la comisión de un presunto delito -autorización que, en el caso de los hechos que se relatarán en esta querella, ni siquiera pareciera haber existido-,

[14].*El escándalo del programa Pegasus desata la sospecha de un estado policial en Israel*.

resulta incompatible con las disposiciones sobre medidas de investigación tecnológica establecidas por la Ley de Enjuiciamiento Criminal [ver, a este respecto los arts. 588 bis a) y siguientes].

IV.II.B.- SOBRE "N.S.O. GROUP"

De denominación legal "N.S.O. GROUP TECHNOLOGIES L.T.D." (en adelante "N.S.O. GROUP"), subsidiaria del grupo de empresas "Q CYBER TECHNOLOGIES"[15] y creadora del software malicioso de inteligencia cibernética al cual se hizo alusión ut supra, la sociedad mencionada es una compañía de desarrollo de tecnología cibernética cuyo slogan de marca es el de ayudar a los servicios de inteligencia y fuerzas de seguridad de los Estados a prevenir e investigar el terrorismo y la delincuencia con el fin de salvar vidas[16]. Sin embargo, como se expondrá más adelante, esa no fue la finalidad de su utilización en los hechos objeto de la presente querella ni en otros muchos que se describen en el cuerpo del presente escrito, por lo que se puede asumir que el objetivo real de dicho sistema de espionaje era y es muy distinto al de evitar o ayudar en la investigación de delitos.

---

[15]. *Israeli spyware company accused of hacking activists hires lobby firm.*

[16] *Complaint NSO, pág. 9.*

"N.S.O. GROUP" fue fundada en la ciudad de Herzliya por los ex agentes del cuerpo de ciberinteligencia del ejército de Israel, Niv KARMI, Shalev HULIO y Omri LAVIE en el año 2010, quienes establecieron esa denominación para la compañía en función de la primera inicial de sus nombres (Niv, Shalev y Omri).

Al iniciar sus operaciones contaron con el apoyo del fondo de inversión GENESIS PARTNERS, que invirtió US$ 1.800.000 en el 30% de sus acciones[17].

En 2011, los ingenieros de "N.S.O. GROUP" finalizaron la codificación de la primera versión de "Pegasus" y poco tiempo después la compañía cerró su primer contrato de venta del software de que se trata con México[18], que habría pagado US$ 20.000.000 por el mismo[19], sin perjuicio de otras cifras muy superiores pagadas desde México en otros momentos de la utilización de dicho sistema de espionaje ilegal.

En 2014, FRANCISCO PARTNERS, una empresa americana de inversión en tecnología, habría pagado US$ 130.000.000 por el 70% de las acciones de "N.S.O. GROUP", y un año después, puso en

---

[17] *El millonario israelí que vende software espía a medio mundo para colarse en tu móvil - El Confidencial*.

[18] *The battle of the most powerful cyberweapon, pág. 9.*

[19] *El millonario israelí que vende software espía a medio mundo para colarse en tu móvil - El Confidencial*.

venta sus acciones por US$ 1.000.000.000[20] lo que refleja la revalorización de la empresa producto de su actividad de espionaje por cuenta de terceros.

En 2019, Shalev HULIO y Omri LAVIE volvieron a adquirir "N.S.O. GROUP" con la ayuda del fondo de inversión londinense, NOVALPINA CAPITAL[21].

De acuerdo a la información de la propia compañía, "N.S.O. GROUP" cuenta con 60 clientes -agencias de inteligencia, divisiones militares y agencias de seguridad estatales- en 40 países, de los cuales no puede revelar su identidad por acuerdos de confidencialidad[22], tratándose de acuerdos de confidencialidad entre partes. Sin embargo, como se pondrá de manifiesto más adelante, dentro de sus clientes también se incluye la comercialización de sus servicios a agencias estatales españolas.

Por su parte, además de "N.S.O. GROUP", "Q CYBER TECHNOLOGIES" cuenta con una subsidiaria en Luxemburgo que fue constituida el 3 de febrero de 2014, de denominación "OSY TECHNOLOGIES S.à.r.l.", cuyo capital social está fijado en US$22.335.078. Entre sus socios, se encuentran

---

[20] *El millonario israelí que vende software espía a medio mundo para colarse en tu móvil - El Confidencial*.
[21] *El millonario israelí que vende software espía a medio mundo para colarse en tu móvil - El Confidencial*.
[22] *Reporte NSO GROUP*.

Shalev HOLY -nominado el 1 de abril de 2019-, Omri LAVIE -nominado el 1 de abril de 2019- y Anthony LEVY -nominado el 25/11/2021-[23].

Estas tres empresas forman el conglomerado que ha operado Pegasus y se han beneficiado de la comercialización de la aplicación y a través de cuyas cuentas bancarias han pasado los pagos por los servicios prestados, incluidos los correspondientes a los hechos objeto de la presente querella.

IV.II.C.- SOBRE EL USO DE "PEGASUS" EN DISTINTOS PAÍSES

A raíz de la investigación periodística "The Pegasus Project", en la que trabajaron más de 80 periodistas de 17 medios de comunicación de 10 países, con la colaboración técnica de Security Lab de Amnistía Internacional, **se ha revelado el uso abusivo del software "Pegasus" por parte de distintos gobiernos clientes de "N.S.O. GROUP" respecto de más de 50.000 números de teléfonos móviles**, entre los cuales se pueden destacar el del presidente de Francia, Emanuel MACRON, el del presidente del Consejo Europeo, Charles MICHEL y el de otros responsables de

[23].*Véase, extracto del Registro de Comercio de Luxemburgo con relación a OSY TECHNOLOGIES.*

estado, funcionarios de gobierno, diplomáticos y oficiales militares de 34 países[24] y, obviamente, entre esos se encuentra el del aquí querellante.

En México, durante la presidencia de Enrique PEÑA NIETO, se ha revelado que la plataforma espía "Pegasus" fue adquirida por parte de la Secretaría de la Defensa Nacional (SEDENA), el Centro de Inteligencia y Seguridad Nacional (CISEN) y la Procuraduría General de la República (PGR) por la suma total de US$ 32.016.000[25].

En ese contexto, también se pudo revelar la creación de al menos 30 empresas "fachada" que estarían ligadas a la red "Pegasus" en México, Panamá y Estados Unidos, así como también transferencias de dinero que se habrían cursado en las sociedades "fachada"[26], entre las que se destacaron pagos de diversas compañías mexicanas a "N.S.O. GROUP" y a las cuentas de Shalev HULIO, uno de los creadores de "Pegasus" y director ejecutivo de la sociedad mencionada[27] -dinámica de ocultación que también se habría implementado en el caso que nos ocupa-.

---

[24].*¿Qué es el Pegasus Project?*.

[25] *Véase Anexos Técnicos del contrato de adquisición de "Pegasus" por parte de la Procuraduría General de la República.*

[26] No es poco habitual que la contratación y uso del sistema Pegasus se realice a través de empresas fachadas para alejar la ilegalidad de su uso de las instancias públicas que realmente habían contratado tales espionajes

[27].*Pegasus Project: la red de empresas que vendió "Pegasus" al gobierno de Peña Nieto*.

En ese mismo país, también se ha constatado su uso para capturar al narcotraficante Joaquín Guzmán Loera ("El Chapo"). Sin embargo, y a pesar de ese concreto uso a efectos de represión de la criminalidad organizada, **también existen informes que indican que ha sido utilizado para fines no legales, como el espionaje de periodistas y de políticos disidentes**[28], razón por la que en México se sigue un proceso penal en contra de diversas personas, algunas de las cuales han sido objeto de medidas cautelares, incluso se ha acordado la prisión provisional. A su vez, se ha informado que **ha sido utilizado para vulnerar las cuentas de quienes apoyaban la sanción del "*impuesto a los refrescos*", como parte de una campaña más amplia contra activistas de derechos humanos, movimientos políticos opositores y periodistas**[29] -finalidad política que, sin duda, ha sido la perseguida en el caso que aquí nos ocupa-.

En cuanto al espionaje de periodistas, al menos 26 de ellos fueron "infiltrados" por el programa "Pegasus" entre el año 2016 y 2017[30]. A su vez, al menos 50 personas del círculo del actual presidente Andrés Manuel LÓPEZ OBRADOR figuran entre las más de 15.000 personas

---

[28].*The battle for the most powerful weapon, pág. 1.*
[29].*The battle for the most powerful weapon, pág. 7, Fuente: Citizen Lab.*
[30].*Quién es quién de las víctimas de los teléfonos infectados por Pegasus, pág. 3.*

seleccionadas como objetivos potenciales de espionaje ilegal en México[31], espionaje a periodistas que también ha sucedido en el presente caso y que seguramente es mucho más amplio del acreditado hasta ahora.

En los Emiratos Árabes Unidos, se ha informado que ha sido utilizado para acceder a los teléfonos móviles de activistas de derechos humanos, personas consideradas como "enemigos" por parte del régimen emiratí[32].

En Arabia Saudita se ha indicado que ha sido utilizado para espiar a activistas feministas, así como también al columnista del Washington Post, Jamal KHASHOGGI, quien fue asesinado el 2 de octubre de 2018 dentro del consulado de Arabia Saudita en Estambul, Turquía, y habiendo sido, aparentemente, calcinados sus restos, en una barbacoa, para evitar dejar pruebas del crimen[33]. Con relación a este último, también se ha informado que, meses antes de su asesinato, Hanan ELATR, una mujer egipcia, la prometida del periodista asesinado, fue espiada mediante "Pegasus", al igual que Hatice CENGIZ, otra pareja del nombrado de nacionalidad turca, que fue víctima de "hackeo" mediante este

---

[31]. Quién es quién de las víctimas de los teléfonos infectadas por Pegasus, pág. 3.
[32]. *The battle for the most powerful weapon, pág. 1.*
[33]. *The battle for the most powerful weapon, pág. 1.*

software de ciberinteligencia escasos días después del crimen del periodista[34].

En Estados Unidos, y debido a que "Pegasus" no tenía la capacidad original de ser utilizado en números de teléfonos móviles americanos, se creó un subsistema del software de ciber inteligencia "Pegasus" denominado "Phantom", que fue testeado por funcionarios del FBI en Nueva Jersey[35]. Sin embargo, en noviembre de 2021, **la Oficina de Industria y Seguridad dependiente del Departamento de Gobierno de Estados Unidos, añadió a "N.S.O. GROUP" al listado de "Malicious Cyber Activities"**, debido a que existirían sobradas evidencias de que los estados extranjeros habrían utilizado indebidamente el software "Pegasus" a los fines de espiar ilegalmente a funcionarios públicos, periodistas, empresarios, activistas, académicos y empleados de embajadas[36].

En Panamá, y durante el gobierno de MARTINELLI, se ha informado que ha sido utilizado para espiar a oponentes políticos, magistrados, líderes sociales y empresarios[37]; debe destacarse que el expresidente MARTINELLI se ha visto envuelto, recientemente y en territorio español, en otro escándalo de espionaje, esta vez de

---

[34]. *Pegasus project: el espionaje de los regímenes autoritarios al desnudo.*.
[35]. *The battle for the most poweful weapon, pág. 2.*
[36] *Demanda Apple NSO, pág. 2.*
[37]. *The battle for the most powerful weapon, pág. 8.*

ámbito familiar en connivencia con cuatro agentes de la Guardia Civil[38].

En Polonia fue adquirido para su Central Anticorrupción y se ha constatado que fue utilizado para espiar ilegalmente, al menos, a 3 miembros de la oposición del gobierno[39].

En India, pese a que ha sido un país que históricamente ha apoyado la causa de Palestina, dicha nación llegó a un acuerdo con Israel en 2017 por u$s 2 billones para la compra de armas de inteligencia -entre las cuales, formaba parte "Pegasus"-[40]. En este país, se ha sabido que "Pegasus" fue utilizado para espiar ilegalmente a Raúl GANDHI, ex presidente del Partido del Congreso Nacional Indio (C.N.I.) y principal rival político del primer ministro, Narendra MODI. Además del recientemente nombrado, también han aparecido como parte de los números telefónicos infectados otros 5 pertenecientes a amigos, familiares y conocidos de GANDHI, así como también de medios críticos al gobierno, como el caso de Siddarth VARADARAJAN y de su socio Paranjoy GUHA THAKURTA[41].

---

[38] Ver, a estos efectos, https://www.abc.es/espana/abci-detienen-cuatro-guardias-mallorca-espiar-novia-expresidente-panama-202203161030_noticia.html

[39]. *The battle for the most powerful weapon, pág. 8. Fuente: Citizen Lab.*

[40]. *The battle for the most powerful weapon, pág. 8.*

[41]. *Quién es quién de las víctimas de lo teléfonos infectados por Pegasus, pág. 3/4.*

En Hungría, se ha informado que el primer ministro de ese país, Viktor ORBAN, ha utilizado "Pegasus" para espiar a personas vinculadas con diferentes medios de comunicación. En concreto, se ha logrado acreditar que el teléfono móvil de la periodista Szabolcs PANYI fue infiltrado al menos durante 7 meses mientras realizaba su investigación periodística sobre la relocalización de un banco ruso a Budapest[42].

En el Reino Unido, se ha informado que la actual directora del periódico Financial Times, Roula KHALAF, nacida en Beirut y con una larga trayectoria profesional como enviada especial a Oriente Próximo y al norte de África, habría sido espiada por el gobierno de Arabia Saudita durante el año 2018[43].

En Marruecos, se ha informado que el periodista de ese país Omar RADI, que ha sido quien ha sacado a la luz informaciones acerca de hechos de corrupción del gobierno de dicho estado, habría sido espiado mediante el programa "Pegasus" entre el año 2018 y el 2019[44].

En Azerbaiyán, se ha informado que la periodista Khadija ISMAYILOVA, que se hizo conocida por sus reportajes de denuncias sobre

---

[42]. *Quién es quién de las víctimas de los teléfonos infectados por Pegasus, pág. 4.*
[43]. *Quién es quién de las víctimas de los teléfonos infectados por Pegasus, pág. 4.*
[44]. *Quién es quién de las víctimas de los teléfonos infectados por Pegasus, pág. 5.*

hechos de corrupción presuntamente cometidos por el régimen autocrático de Ilham ALIYEV, fue espiada mediante el software de inteligencia cibernética "Pegasus" en el año 2019[45].

En Ruanda, se ha informado que Carinae KANIMBA -hija del activista encarcelado Paul RUSESABAGINA-, que se ha puesto al frente de la campaña para liberar a su padre y ha criticado fuertemente el régimen del presidente Paul KAGAME, fue sometida a una operación de vigilancia con la ayuda del programa "Pegasus"[46].

En El Salvador, a raíz de una investigación conducida por The Citizen Lab y Access Now, con colaboración de Frontline Defenders, SocialTIC y Fundación Acceso, se ha confirmado que, entre julio de 2020 y noviembre de 2021, "Pegasus" fue utilizado para espiar ilegalmente a periodistas de diferentes medios de comunicación de ese país, tales como El Faro, GatoEncerrado, La Prensa Gráfica, Revista Digital Disruptiva, Diario El Mundo, El Diario de Hoy, así como también a periodistas independientes y a miembros de las sociedades civiles Fundación DTJ y Cristosal, entre otras[47].

---

[45]. *Quién es quién de las víctimas de los teléfonos infectados por Pegasus, pág. 5.*
[46]. *Quién es quién de las víctimas de los teléfonos infectados por Pegasus, pág. 5.*
[47] *Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvado with "Pegasus" Spyware - The Citizen Lab.*

Del informe citado en el párrafo que antecede no sólo se concluye que los dispositivos móviles de los periodistas y miembros de sociedades civiles fueron accedidos ilegalmente mediante "Pegasus", sino también que existiría evidencia forense relativa a que se habría logrado extraer información de aquellos dispositivos hacia la infraestructura de "Pegasus", dicho más claramente: **información trasladada a los servidores de la empresa "N.S.O. GROUP" en Israel o en algún otro país, que es lo que también habría sucedido, en principio, en el presente caso.**

Si bien por el informe anterior se pone de manifiesto que no resulta posible atribuir de forma concluyente la autoría de los ataques cibertecnológicos referidos a un Estado-Cliente de "N.S.O. GROUP" en particular, lo cierto es que, de todos modos, se puntualiza que existiría una fuerte evidencia circunstancial para pensar que el gobierno de El Salvador podría estar detrás de los mismos, esto es, el gobierno del presidente Nayib Armando BUKELE ORTEZ. Esto es así, pues, casualmente, todos los ataques mediante este software de ciberinteligencia tienen el denominador común de que fueron dirigidos contra personas que se encontraban, en esos precisos momentos, trabajando en asuntos de sumo interés para el gobierno de BUKELE ORTEZ

-tales como los datos que revelaron el escandaloso pacto que el gobierno de El Salvador habría acordado con la organización terrorista "MS-13"[48]-.

En el caso que nos ocupa, y a partir de la publicación por parte de la revista norteamericana The New Yorker de un extenso reportaje sobre el espionaje a políticos catalanes, se han realizado manifestaciones públicas que indican que efectivamente los clientes de "N.S.O. GROUP", en este caso, son personas de nacionalidad española, pendientes de identificar, y que habrían actuado amparándose en el indebido uso de sus respectivas posiciones como miembros de cuerpos y fuerzas de seguridad del Estado[49].

Los anteriores son algunos de los documentados ejemplos sobre las criminales actividades desplegadas en diversos países por parte de "N.S.O. GROUP" y diversas agencias estatales de los países antes nombrados, tal cual, como veremos *ut infra*, ha sucedido en España.

IV.II.D.- CONTEXTO EN EL QUE SE PERPETRAN ESTOS DELITOS

[48]. *Bukele pactó con la pandilla M-13 en El Salvador*.
[49] *How Democracies Spy on their Citizens*.

Los acontecimientos que se pondrán de manifiesto en este apartado, pondrán en evidencia la innumerable cantidad de medidas adoptadas por diversos estamentos del Estado español, especialmente desde las altas instancias jurisdiccionales así como por parte de radicales sectores dentro de las Fuerzas y Cuerpos de Seguridad del Estado, con el fin de reprimir el derecho a la participación política del Sr. Carles PUIGDEMONT, el Sr. Antoni COMIN, la Sra. Clara PONSATÍ y el Sr. Lluís PUIG, entre otros líderes independentistas catalanes, hechos que no pueden ser pasados por alto como línea de investigación a los fines de entender y dimensionar la gravedad de los sucesos delictivos que se denunciarán más adelante.

El Sr. Carles PUIGDEMONT fue presidente de Catalunya desde el 10 de enero de 2016 y hasta que fue depuesto el 27 de octubre de 2017. El Sr. Antoni COMIN fue consejero de Salud del gobierno del Sr. PUIGDEMONT desde el 14 de enero de 2016 hasta que fue depuesto el 27 de octubre de 2017. La Sra. Clara PONSATÍ fue consejera de Educación del gobierno del Sr. PUIGDEMONT desde el 14 de enero de 2016 hasta que fue depuesta el 27 de octubre de 2017. El Sr. Lluís PUIG fue consejero de Cultura del gobierno del Sr. PUIGDEMONT desde

el 5 de julio de 2017 hasta que fue depuesto el 27 de octubre de 2017.

En esa última fecha, y luego de las idas y vueltas entre la intención del Parlamento de Catalunya de iniciar un proceso institucional de independencia y las consecuentes decisiones del Tribunal Constitucional, todas ellas a raíz de lo postulado en ese sentido por el gobierno de España (proceso que, en lo que interesa a la presente, cabe delimitar desde la sentencia del Tribunal Constitucional Español del 9 de julio de 2010, por la cual se impugnó el Estatuto de Autonomía de Catalunya, hasta la decisión del Parlamento catalán que declaró la independencia el 27 de octubre de 2017 -que tuvo sustento en el referéndum celebrado en Catalunya el 1° de octubre del mismo año-, pese a la decisión en contrario del Tribunal Constitucional), el presidente de aquel gobierno, Mariano RAJOY, con el acuerdo del senado español, disolvió el parlamento catalán, impuso el gobierno directo en virtud del art. 155 de la Constitución Española y convocó inmediatamente nuevas elecciones al Parlamento de Catalunya para el 21 de diciembre de 2017.

Esto implicó la destitución de todo el gobierno catalán, incluidos el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ y el Sr. Lluís PUIG -primera medida de extinción del derecho a la

participación política- y el inicio de una extensa persecución política -mediante una indebida utilización del poder judicial y del Tribunal Constitucional- fomentada por el gobierno español contra los nombrados, entre otros líderes independentistas catalanes, con el objetivo de extinguir su derecho a la participación política.

Además de haberles quitado la posibilidad de ejercer los cargos por los cuales fueron oportunamente electos, el Sr. Carles PUIGDEMONT, el Sr. Antoni COMIN, la Sra. Clara PONSATÍ y el Sr. Lluís PUIG fueron denunciados penalmente con la intención de que no les sea posible ejercer cargos públicos en Catalunya y en ninguna institución de España, pese a que los mencionados mantenían el apoyo popular de una mayoría de la población en cada elección[50].

En concreto, el 30 de octubre de 2017, el Fiscal General del Estado español presentó querella por la comisión de rebelión, sedición y malversación de fondos públicos en la Audiencia Nacional contra el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ, el Sr. Lluís PUIG y otros políticos independentistas catalanes. Se ignoraba así la denuncia previa presentada con cargos

[50] *Prueba del apoyo popular, es que aquél fue utilizado por el juez investigador del Tribunal Supremo para mantener detenidos preventivamente a miembros del ex gobierno del Sr. PUIGDEMONT a la espera del juicio respectivo.*

menos graves ante el Tribunal Superior de Justicia de Catalunya, tribunal competente para conocer de las acusaciones penales contra los miembros del Gobierno catalán y del Parlamento de Catalunya. La Fiscalía justificó que era más *"conveniente"* presentar la querella contra el gobierno del Sr. PUIGDEMONT en Madrid, como ocurre, dijo, con las acusaciones penales sobre terrorismo.

Desde el inicio del procedimiento contra el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ y el Sr. Lluís PUIG, el Ministerio Fiscal indicó que, tras la disolución del Parlamento de Catalunya, el Sr. PUIGDEMONT (junto con sus ministros) ya no gozaba de inmunidad como miembro del Gobierno o del Parlamento de Catalunya. El 31 de octubre de 2017, la Audiencia Nacional se declaró competente para conocer la querella contra el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ, el Sr. Lluís PUIG y el resto del Gobierno catalán, y los citó a comparecer dos días después. Las citaciones nunca fueron notificadas a los Sres. PUIGDEMONT, COMIN, PONSATÍ y PUIG GORDI. Tal y como reconoció públicamente el 23 de enero de 2018 el entonces ministro del Interior de España, D. Juan Ignacio Zoido (hoy eurodiputado), en el momento en que el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ y el Sr. PUIG GORDI se exiliaron el 29 de octubre

de 2017, nada podía impedirlo legalmente[51], dado que ningún procedimiento penal se había dirigido en su contra en esas fechas.

La defensa de los señores PUIGDEMONT, COMIN, PONSATÍ y PUIG GORDI compareció ante la Audiencia Nacional y solicitó que aquellos imputados que se encontraban en Bélgica pudieran ser oídos por videoconferencia, tal y como se contempla tanto en la Ley de Enjuiciamiento Criminal española como en el artículo 1.3 de la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal[52]. El juez de instrucción denegó la petición al considerar que no existía soporte legal para dicha petición. Es importante señalar que este tipo de peticiones se han presentado en varias ocasiones en los últimos tres años y siempre han sido desestimadas por los tribunales españoles.

La jueza del Juzgado Central de Instrucción N° 3, de la Audiencia Nacional, Carmen LAMELA[53], a petición del fiscal del Estado,

---

[51] *El Sr. Zoido dijo: "...El Sr. PUIGDEMONT cuando salió de España no tenía ningún tipo de medida que le impidiera actuar con absoluta libertad. No tenía ninguna restricción de la misma, ni ninguna orden que permitiera que se le vigilara. Por tanto, él salió en uso de su derecho de España. A continuación es cuando se han producido ya todas las actuaciones...". Véase, a tal efecto, Entrevista al Sr. Zoido en Antena 3, minuto 6:30.*

[52] *De conformidad con el artículo 36, apartado 1, de la Directiva 2014/41, el plazo de transposición expiró el 22 de mayo de 2017.*

[53] *Carmen Lamela fue posteriormente nombrada magistrada del Tribunal Supremo español, en lo que algunos consideraron una recompensa por su papel en el procesamiento de los líderes independentistas.*

ordenó prisión sin fianza para todos ellos, excepto para uno. El auto de prisión consideró que habían tenido tiempo suficiente para preparar su defensa, a pesar de que la acusación les fue notificada sólo unas horas antes.

El 3 de noviembre de 2017 el juez de instrucción de la Audiencia Nacional emitió órdenes europeas de detención y entrega contra el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ, el Sr. Lluís PUIG y la Sra. Meritxell SERRET, que se encontraban presentes en Bruselas, tras su inasistencia a la vista del día anterior en Madrid.

El 5 de noviembre de 2017 las cinco personas mencionadas precedentemente, acompañados de sus abogados, se presentaron ante la policía belga. Tras una audiencia de diez horas, un juez belga los puso en libertad. Se les ordenó que no salieran de Bélgica sin permiso y que facilitaran los datos de su alojamiento.

El 24 de noviembre de 2017, el juez instructor del Tribunal Supremo, D. Pablo LLARENA, que llevaba la investigación por rebelión y sedición contra los miembros de la Mesa del Parlamento de Catalunya, ordenó la acumulación de dicha investigación a las iniciadas en la Audiencia Nacional y en el Tribunal Superior de Justicia de Catalunya. Lo

hizo a pesar de que dos días antes, el 22 de noviembre de 2017, incluso el Ministerio Fiscal le había recordado que, de acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos, tal decisión podría vulnerar el derecho a un tribunal previamente establecido por la ley en virtud del artículo 6 del Convenio.

El 5 de diciembre de 2017, el Tribunal Supremo español, por razones que fueron calificadas de *"estratégicas"*, retiró la primera orden europea de detención y entrega contra el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ, el Sr. Lluís PUIG y la Sra. Meritxell SERRET, por considerar que, a su juicio, la previsible negativa a ejecutar esa orden de detención europea en sus propios términos por parte de las autoridades belgas podría poner en peligro la investigación contra un grupo más amplio de personas, es decir, los consejeros del gobierno catalán encarcelados o perseguidos en España. Sin embargo, el juez de instrucción Sr. LLARENA advirtió que las órdenes de detención nacionales seguirían siendo válidas a pesar de la retirada de la orden de detención europea, lo que significa que el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ, el Sr. Lluís PUIG se enfrentarían a la detención y a la prisión preventiva si retornaban a España.

A pesar de ser depuestos en su momento, el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ y el Sr. Lluís PUIG se presentaron como candidatos a las elecciones al Parlamento de Catalunya del 21 de diciembre de 2017 desde Bélgica y fueron reelegidos como diputados. El partido del gobierno nacional, el Partido Popular, sufrió una reducción del 50% de sus votos hasta el 4,2%. Los partidos independentistas mantuvieron su mayoría parlamentaria. El Sr. PUIGDEMONT fue propuesto como futuro Presidente por una mayoría absoluta del Parlament de Catalunya, pero el Gobierno español, en su afán de continuar lesionando el derecho del nombrado a la participación política, se negó a aprobar su regreso al cargo, sugiriendo en su lugar que el Parlamento catalán presentara un *"candidato limpio"*[54].

Tras las elecciones, concretamente el 17 de enero de 2018, el Parlamento catalán eligió una nueva Mesa, formada por una mayoría de diputados independentistas. Esto formaba parte de un acuerdo entre tres partidos políticos para respaldar al Sr. PUIGDEMONT como candidato a Presidente antes de la primera votación oficial sobre la elección, que debía tener lugar antes del 31 de enero de 2018. El Presidente del Parlamento nombró oficialmente al Sr. PUIGDEMONT

[54] Rajoy pide un "candidato limpio" para la generalitat. ABC.

como candidato a la investidura a Presidente de la Generalitat el 23 de enero, y convocó una sesión parlamentaria para el debate y la elección para el 30 de enero de 2018.

El 22 de enero de 2018, el juez de instrucción del Tribunal Supremo español decidió no dictar una nueva orden europea de detención y entrega contra el Sr. PUIGDEMONT, quien se hallaba de viaje en Dinamarca,desatendiendo la petición de la Fiscalía, por el motivo explícito de que dictar una nueva orden de detención europea contra él podría beneficiar a la actividad política del Sr. PUIGDEMONT, concretamente a sus posibilidades de ser reelegido como Presidente.

El gobierno español solicitó al Tribunal Constitucional, el 26 de enero de 2018, que prohibiera la sesión del Parlamento catalán para reelegir al Sr. PUIGDEMONT como presidente. La vicepresidenta del Gobierno español declaró que las circunstancias no permitían que el Parlamento eligiera al Sr. PUIGDEMONT, ya que no gozaba de sus plenos derechos y *"no tenía derecho a la libertad de circulación".*

En otro episodio de evidente intención de anular el derecho a la participación política del Sr. PUIGDEMONT, a las 21:00 horas del sábado 27 de enero de 2018, el Tribunal Constitucional

acordó por unanimidad dictar una medida cautelar que suspendía cualquier sesión del parlamento catalán convocada para la reelección del Sr. PUIGDEMONT, salvo que compareciera personalmente con una autorización judicial previa. También declaraba que la comparecencia personal no podía ser sustituida por una delegación en otro diputado o por medio de la telecomunicación[55], así como también la nulidad de cualquier resolución que el Parlamento catalán pudiera adoptar en contra de su requerimiento previo y la advertencia a los miembros de la Mesa del Parlamento de Catalunya que si no hacían cumplir la decisión del Tribunal iban a tener consecuencias penales.

El 1 de marzo de 2018, el Parlamento de Catalunya aprobó una resolución en la que se confirmaba que una mayoría global deseaba reelegir al Sr. PUIGDEMONT como Presidente y pedía a las autoridades españolas que desistieran de sus intentos de bloquear arbitrariamente la realización de la voluntad democrática de los votantes que apoyan a los partidos que respaldan

[55] *En consecuencia, el Sr. PUIGDEMONT presentó una solicitud de autorización para asistir a la sesión parlamentaria. La solicitud se dirigió al juez competente del Tribunal Supremo español. El juez, sin embargo, no estaba dispuesto a considerar la solicitud sin la presencia física del Sr. PUIGDEMONT en la sala. Su presencia física, por supuesto, habría conducido inevitablemente a su detención inmediata y a su encarcelamiento arbitrario, ya que ha estado todo el tiempo sujeto a una orden de detención interna por rebelión y sedición. Su destino habría sido inevitablemente el mismo que el de los demás miembros destacados de su Gobierno, en particular el Sr. Junqueras, que se encuentra en detención arbitraria desde noviembre de 2017.*

al Sr. PUIGDEMONT. Sin embargo, el gobierno español no desistió, por lo que el Sr. PUIGDEMONT se vio obligado a apartarse como candidato a Presidente de la Generalitat. Este era el único paso que le quedaba para evitar el bloqueo permanente del Parlament y la extensión del dominio directo del Gobierno español sobre Catalunya.

El 23 de marzo de 2018, el juez de instrucción del Tribunal Supremo también hizo pública su decisión, adoptada el 21 de marzo, de dictar auto de procesamiento,o confirmar el proceso penal contra el Sr. PUIGDEMONT, el Sr. SÁNCHEZ, el Sr. TURULL y otras diez personas por actos de rebelión relacionados con la organización del referéndum de independencia del 1º de octubre de 2017 (incluidos el Sr. COMIN, la Sra. PONSATÍ y el Sr. Lluís PUIG). También imputó a otros once políticos por delitos de desobediencia y malversación de fondos públicos.

La imputación sustentada desde la perspectiva del delito de rebelión -entre otros delitos- no es una cuestión menor, toda vez que resultó un medio idóneo para suspender de sus cargos públicos a 12 de los dirigentes catalanes, entre ellos los Sres. PUIGDEMONT y COMIN, sin una condena previa.

En este sentido, el Tribunal Supremo aplicó el artículo 384 *bis* de la Ley de Enjuiciamiento Criminal española[56], que prevé este tipo de suspensión sólo para terroristas y rebeldes. De esta manera, consiguieron forzar la salida de sus cargos a quienes no los habían abandonado voluntariamente. La señora PONSATÍ ya había dejado su cargo de diputada en el Parlamento de Catalunya el 29 de enero de 2018 y se había reincorporado a su cátedra en la Universidad de St Andrews (Escocia). Además, el juez decidió emitir una segunda orden de detención europea contra el Sr. PUIGDEMONT, el Sr. COMIN, la Sra. PONSATÍ, el Sr. Lluís PUIG y la Sra. Meritxell SERRET, que se encontraban exiliados en Bruselas.

El 25 de marzo de 2018, el Sr. PUIGDEMONT fue detenido en Alemania a su regreso a Bélgica desde Finlandia. Pasó 12 días en prisión preventiva, hasta el 5 de abril de 2018, cuando fue puesto en libertad bajo fianza. El tribunal alemán descartó la entrega a las autoridades españolas por cargos de rebelión ya que el delito equivalente en el código penal alemán requería una violencia real y sustancial, que no se había producido en el caso del Sr. PUIGDEMONT.

[56] El artículo 384 *bis de la* Ley de Enjuiciamiento Criminal española establece: "*Cuando la acusación, unida a la prisión preventiva, respecto de una persona que forma parte o está relacionada con bandas armadas o individuos terroristas o rebeldes es definitiva, el acusado que esté ocupando una función o cargo público queda automáticamente suspendido en el ejercicio de éste mientras permanezca detenido*."

El 26 de abril de 2018, el Tribunal Constitucional emitió su decisión sobre la impugnación del gobierno español contra la convocatoria de la sesión electoral parlamentaria de enero de 2018 en la que debía ser elegido el Sr. PUIGDEMONT. Concretamente, el tribunal admitió la impugnación, suspendió la convocatoria de la sesión parlamentaria, declaró nula cualquier resolución que pretendiera volver a proponer al Sr. PUIGDEMONT y advirtió a los miembros de la Mesa del Parlament que serían perseguidos penalmente si lo proponían de nuevo y/o permitían su elección[57].

Es importante señalar que finalmente no se condenó a nadie por el delito de rebelión y el Tribunal Supremo tuvo que admitir que la suspensión del señor PUIGDEMONT como diputado del Parlamento catalán carecía de toda base legal y tuvo que ser revocada. Sin embargo, como confesó el juez instructor en un discurso pronunciado el 22 de noviembre de 2019 (poco después de levantar la suspensión), ésta había servido para inhabilitar a los dirigentes catalanes para el

[57] *Esta decisión se basó en el apartado 2 del artículo 161 de la Constitución española, que prevé la suspensión automática de las disposiciones cuando son impugnadas por el Gobierno español. El Sr. PUIGDEMONT, así como todos los miembros del Parlamento catalán pertenecientes a su partido, habían argumentado que la suspensión de la sesión electoral vulneraba la autonomía y la inviolabilidad del Parlamento, el principio de separación de poderes y los derechos fundamentales protegidos por las Constituciones, así como los derechos establecidos en los artículos 19, 21, 22 y 25 del PIDCP. El propio Parlamento de Catalunya presentó un recurso similar. El Tribunal Constitucional desestimó estos argumentos.*

ejercicio de cargos públicos antes de que se probara ninguna de las acusaciones que se les imputaban[58].

Otro elemento a tener en cuenta para valorar la infundada acusación del delito de rebelión, artilugio legal utilizado para suspender en sus cargos públicos a los ex miembros del gobierno catalán mientras durara el proceso, fue que el 14 de octubre de 2019 el Tribunal Supremo dio a conocer su Sentencia N° 459/2019 en el proceso penal contra ex miembros del Gobierno catalán y activistas sociales. En ese proceso, si bien el tribunal condenó a nueve de ellos como autores de un delito de sedición y a algunos de ellos también por malversación de fondos públicos, resulta relevante remarcar que aquéllos **fueron absueltos de los cargos de rebelión que habían sido la base de su suspensión de los cargos públicos antes de ser condenados**.

Dado que los derechos del Sr. PUIGDEMONT, el Sr. COMIN y la Sra. PONSATÍ a participar en el Gobierno y en las instituciones de su país a través de elecciones democráticas fue absolutamente socavado, el 10 de marzo de 2019 los nombrados decidieron finalmente presentarse a las elecciones al Parlamento Europeo, convencidos de que esta institución era la última y única en

[58] *Conferencia pública de D. Pablo Llarena Conde, magistrado instructor del Tribunal Supremo, celebrada el 22 de noviembre de 2019 en la sede del Tribunal Superior de Justicia de Castilla y León, minuto 44:10.*

la que podrían representar a su pueblo. Sin embargo, como se detallará, el gobierno de España y el Parlamento Europeo se confabularon para continuar la campaña destinada a excluirlos de la vida pública, lo que tuvo lugar hasta que el Tribunal de Justicia de la Unión Europea se pronunció sobre la ilegalidad de dicha exclusión los días 19 y 20 de diciembre de 2019[59].

En este contexto, las autoridades españolas, junto con sus adversarios políticos, intentaron primero excluirlos como candidatos a las elecciones europeas celebradas el 26 de mayo de 2019[60].

---

[59] *Aquí cabe agregar que, pese a que con motivo de aquella decisión el Parlamento Europeo concedió el derecho a los nombrados para que tomen posesión de sus escaños como diputados, el Tribunal Supremo español se negó a acatar la sentencia del Tribunal de Justicia sobre la inmunidad y, en su lugar, el magistrado instructor decidió el 10 de enero de 2020 mantener las órdenes de prisión y de detención europea emitidas ilegalmente contra el Sr. PUIGDEMONT y el Sr. COMIN después de que fueran elegidos. Ese mismo día, el Tribunal también emitió este suplicatorio de suspensión de la inmunidad del Sr. PUIGDEMONT y del Sr. COMIN con el único fin de ejecutar esas órdenes ilegales de prisión y extradición e impedirles ejercer su cargo electo. Las autoridades judiciales españolas siguieron ignorando las sentencias del Tribunal de Justicia tras la proclamación de la Sra. PONSATÍ como diputada al Parlamento Europeo el 23 de enero de 2020. Así, el Tribunal Supremo español rechazó suspender el procedimiento contra la Sra. PONSATÍ y emitió un suplicatorio de suspensión de su inmunidad los días 3 y 4 de febrero de 2020.*

[60] *El 25 de abril de 2019 el Partido Popular-EPP y Ciudadanos-Renovación presentaron una reclamación contra la inclusión de los señores PUIGDEMONT, COMIN y PONSATÍ en la lista de candidatos Lliures per Europa (Junts) que había sido enviada a la Junta Electoral Central española, junta que decidió ilegalmente excluirlos de la lista -entre los miembros de la Junta Electoral Central española que votaron para excluirlos como candidatos había una persona que posteriormente se demostró que estaba en la nómina de Ciudadanos, el partido del actual Presidente de la Comisión de Asuntos Jurídicos del Parlamento Europeo, el Sr. Adrián Vázquez-. Esta cuestión tuvo final en la justicia en lo contencioso-administrativo, en donde se falló a favor de los afectados, permitiéndoles optar a un escaño en el Parlamento Europeo.*

Paralelamente al intento de impedir que se presentaran como candidatos al Parlamento Europeo, se desplegó una segunda estrategia que tenía la misma finalidad ilegítima: impedir que el Sr. PUIGDEMONT, el Sr. COMIN y la Sra. PONSATÍ fueran elegidos diputados del Parlamento Europeo. Esta vez, utilizando los Servicios del Parlamento Europeo para intentar engañar a los votantes catalanes, haciéndoles creer que los nombrados no eran candidatos legalmente viables [61].

Después, una vez elegidos y en un hecho que puede ser calificado sin precedentes, el Sr. PUIGDEMONT y el Sr. COMIN fueron privados de su derecho a tomar posesión de sus escaños, al exigirles España y el Parlamento que acudieran primero a Madrid para prestar juramento de fidelidad a la Constitución española[62].

Ante el temor de que esto no les impidiera tomar posesión de sus escaños a largo plazo, las autoridades judiciales emitieron otra orden de *"búsqueda, detención y envío a prisión"*

---

[61] *El entonces presidente del Parlamento Europeo, Antonio TAJANI, en un hecho sin precedentes, solicitó en secreto un dictamen al Servicio Jurídico del Parlamento Europeo en relación a si los mencionados podían presentarse en las elecciones y si, en caso de ser elegidos, podían adquirir la plena condición de diputados. Este informe, fue filtrado adrede en la prensa para generar la impresión pública de que los afectados no eran candidatos legalmente viables.*

[62] *Al requisito necesario para ser eurodiputado de prometer lealtad a la Constitución Española, le añadieron un prerrogativa no prevista por la ley: que la promesa tuviera que hacerse en persona, en Madrid, ello a los fines de obligar a los mencionados a presentarse en España para ser detenidos por los cargos en su contra y ser impedidos de ejercer su derecho a la participación política.*

de los tres eurodiputados electos[63]. Se trataba de la tercera orden de detención europea, por los mismos hechos, desde que se inició el procedimiento contra ellos en 2017.

En este sentido, y antes de que el Tribunal de Justicia pudiera tomar una decisión sobre si el Parlamento Europeo tenía que reconocer al Sr. PUIGDEMONT, al Sr. COMIN y a la Sra. PONSATÍ como diputados, el 10 de octubre de 2019, la Fiscalía presentó una solicitud secreta ante el juez de instrucción del Tribunal Supremo español para que emitiera una nueva orden de detención europea contra el señor PUIGDEMONT. Tras haberlo solicitado en noviembre de 2017, en enero de 2018 y en marzo de 2018, esta era la cuarta ocasión en la que el Ministerio Público se lo pedía al juez instructor. Pero esta vez la petición era manifiestamente ilegal: el señor PUIGDEMONT era diputado desde el 13 de junio de 2019. Llamativamente, la petición se basaba en el supuesto de que **cuatro días después** varios exconsejeros del gobierno del señor PUIGDEMONT serían condenados por sedición y malversación de fondos públicos por el Tribunal Supremo español.

Consecuentemente, el 14 de octubre de 2019, el Tribunal Supremo español hizo pública su sentencia en la que condenaba a los miembros del

[63] *Como veremos, la Sra. PONSATÍ era la siguiente en la lista para convertirse en eurodiputada si finalmente se aplicaba el Brexit.*

anterior Gobierno catalán por sedición y malversación de fondos públicos a penas de entre 5 y 13 años de prisión y, en la misma fecha, el juez de instrucción del Tribunal Supremo español, basándose en dicha sentencia, dictó nuevas órdenes de detención nacionales y europeas ilegales contra el Sr. PUIGDEMONT. Se había iniciado el tercer procedimiento de entrega en virtud del capítulo 2 de la Decisión marco 2002/584, pese a que el nombrado era diputado del Parlamento Europeo desde el 13 de junio de 2019.

Como consecuencia de esta medida, el Sr. PUIGDEMONT fue detenido en Bélgica el 17 de octubre de ese año, siendo puesto en libertad el 18 de octubre, sujeto a la prohibición de abandonar el país, y teniendo que estar localizable en todo momento.

Sin embargo, tras el dictado de la sentencia del Tribunal de Justicia en el asunto C-502/19, el 19 de diciembre de 2019, por la cual aquel tribunal reconoció a PUIGDEMONT y a COMIN como diputados del Parlamento Europeo, el juez de primera instancia belga decidió suspender el procedimiento, reconociendo esa condición.

Finalmente, el 6 de enero de 2020 el Parlamento Europeo reconoció por primera vez a PUIGDEMONT y a COMIN como eurodiputados,

haciéndolo con efecto retroactivo a partir del 2 de julio de 2019.

Como una prueba final de la vulneración de las inmunidades de los afectados, y pese a la decisión del Tribunal de Justicia, en un último disparo sin escrúpulos para impedir que el Sr. PUIGDEMONT, el Sr. COMIN y la Sra. PONSATÍ ejerzan su labor como diputados al Parlamento Europeo, y continuar la persecución política contra ellos, el Tribunal Supremo, sin perjuicio de reconocer la inmunidad parlamentaria que los nombrados podían tener en toda la Unión Europea, en un auto de 10 de enero de 2020, estableció, sin base legal alguna, que aquella inmunidad no era aplicable en España. En esa misma fecha, aquel tribunal dictó un auto en el que decidió mantener las órdenes de detención nacional y europea contra los señores PUIGDEMONT y COMIN, y solicitó al Parlamento Europeo la suspensión de su inmunidad en relación con el apartado b) del párrafo primero del artículo 9 del Protocolo.

Por último, el 23 de septiembre de 2021, el M.H.P. Puigdemont es detenido en Italia, por orden del Juez del Tribunal Supremo D. Pablo Llarena, cuando acudía a dicho país en su condición de eurodiputado; su detención se produjo como consecuencia de un incumplimiento de las normas establecidas en el Estatuto del

Tribunal de Justicia de la Unión Europea por parte del Juez Llarena que no había suspendido las euro órdenes como es preceptivo.

En un primer momento se informó, por parte de las autoridades españolas, que la detención se habría producido tras ser informados del viaje por las autoridades italianas, posteriormente se cambió la explicación y surgió una nueva según la cual su viaje y detención estaba siendo monitorizado por altos mandos del Cuerpo Nacional de Policía desde Valladolid, sin haber explicando núnca en qué consistía dicho monitoreo.

Todos estos acontecimientos deberán ser tenidos en cuenta a los fines de investigar los hechos que se denunciarán por esta querella porque forman parte del contexto político en el cual se diseña, establece y ejecuta el sistemático espionaje al que ha sido sometido el querellante, abogado en ejercicio, y otros, mayoritariamente miembros de la minoría nacional catalana.

A partir del anterior contexto, debe tenerse presente aquél que más específica y directamente afecta al aquí querellante.

En este sentido, cabe mencionar que, desde el 29 de octubre de 2017, el Sr. Gonzalo

BOYE defiende a varios de los miembros del depuesto Govern de Catalunya hoy en el exilio y coordina la defensa internacional de los mismos. Esta coordinación abarca la formación de un equipo internacional de abogados en Escocia, Bélgica, Francia, Alemania e Italia.

El querellante ha logrado coordinar el trabajo más exitoso hasta la fecha en defensa de quienes han visto criminalizada su actividad política relacionada con su ideología y anhelo independentista.

Estos éxitos han consistido en impedir, con un equipo jurídico internacional, que varias OEDE cursadas por las autoridades judiciales para la entrega de los exiliados fuesen finalmente ejecutadas.

Junto con esta actividad antes expuesta, debemos destacar también, que el querellante dirige la estrategia de defensa de los antes mencionados en los diversos procesos que se siguen ante el Tribunal de Justicia de la Unión Europea y ante el Tribunal General de la Unión Europea así como el previo procedimiento de suplicatorio tramitado por el Parlamento Europeo.

Durante todo ese tiempo, el querellante ha sido víctima de los hechos que se describen *ut infra* así como durante el tiempo en que ha estado

llevando las defensas de otros muchos políticos catalanes, convirtiéndose en objetivo de campañas de desprestigio, infundadas acusaciones incluso penales y, ahora, demostrándose víctima de un espionaje como el que se describirá.

V.- BREVE RESUMEN DE LOS HECHOS OBJETO DE LA PRESENTE QUERELLA

A raíz del informe emitido recientemente por The Citizen Lab[64], se puso en evidencia y se pudo acreditar que, a partir del año 2017 -y posiblemente también desde el año 2015- al menos 65 personas[65] fueron infectadas o atacadas con el software espía "Pegasus" dentro del estado español.

Entre estas personas se encuentra el abogado ejerciente D. Gonzalo BOYE que, entre otras, participa en la defensa de:

- El expresidente catalán el M.H.P. Carles PUIGDEMONT,
- El expresidente catalán M.H.P. Quim TORRA,

[64] *Véase, informe completo y gráfico "Catalan Gate".*
[65] Seguramente en los próximos meses esta cifra se verá notablemente incrementada en la medida en que avancen los análisis forenses de los dispositivos de otros muchos ciudadanos espiados ilegalmente.

- La M.H.P. del Parlament de Catalunya Laura BORRÁS,
- Los eurodiputados D. Antoni COMIN y Dña. Clara PONSATÍ, el diputado D. Lluís PUIG,
- Las diputadas Míriam NOGUERAS I CAMERO y Mariona ILLAMOLA DAUSÀ,
- Los senadores María Teresa RIVERO I SEGALÀS, Josep Lluís CLERIES I GONZÀLEZ, Josep María MATAMALA ALSINA, Assumpció CASTELLVÍ AUVÍ y Josep María CERVER PINART,
- Los señores D. Josep Lluís ALAY y D. Lluís ESCOLA, y
- El cantante D. Josep Arenas BELTRAN (Valtonyc) -exiliado también en Bélgica-.

Concretamente, de acuerdo a lo que se ha determinado ya en el informe forense emitido por The Citizen Lab, entre enero y mayo del año 2020 el abogado D. Gonzalo BOYE fue víctima de al menos 18 ataques mediante la utilización del software espía "Pegasus", a través de mensajes SMS que contenían un enlace "malicioso" ("malware"), disfrazado de notificaciones de Twitter relacionadas con supuestos "tuits" de organizaciones como:

- La ONG de derechos humanos "Human Right Watch",
- el diario "The Guardian",

- la revista “Columbia Journalism Review”, o
- la revista “Político”.

Es decir, todos procedentes de organizaciones o medios de comunicación con los que contacta habitualmente mi representado o que lee de forma regular el aquí querellante.

El análisis forense realizado sobre el teléfono móvil de mi representado encontró, además, evidencia concluyente con respecto a otra infección activada mediante la utilización del software espía “Pegasus” al 30 de octubre de 2020, desconociéndose, por el momento, cuánto tiempo estuvo activado el espionaje sobre su dispositivo móvil pero, al igual que los otros 18, todo ello coincide con relevantes eventos a efectos profesionales del querellante, como Letrado en ejercicio.

La fecha en la que se produjeron los ataques a través de este programa espía no resultan casuales, si se tiene en consideración que tan solo 48 horas antes de producida aquélla había sido arrestado, entre otras personas, D. Josep Lluís ALAY, defendido de D. Gonzalo BOYE, ex coordinador de Políticas Internacionales durante la presidencia del Gobierno del M.H.P. Quim TORRA y en ese momento director de la

oficina del M.H.P. Carles PUIGDEMONT, en el marco de lo que se denominó la "Operación Vóljov"[66].

Asimismo, tampoco puede pasarse por alto que, en la época en la que se produjeron los diversos ataques al dispositivo móvil de mi defendido mediante la utilización de "Pegasus" -entre enero y mayo de 2020-, así como también la infección a través de este programa espía a partir del 30 de octubre de 2020, mi representado estuvo participando, debido a diversas restricciones sanitarias como consecuencia de la pandemia, en complicadas y constantes videoconferencias tanto con el expresidente Carles PUIGDEMONT y el expresidente Quim TORRA como con otros defendidos, entre los que se encontraban muchos otros políticos catalanes, así como también estuvo en contacto profesional con los abogados de Bélgica, Escocia y Alemania con los que lleva adelante la defensa de los políticos catalanes exiliados en esos países y otros casos no menos relevantes.

Por mencionar solo algunos de los eventos relacionados con el espionaje sufrido entre enero y mayo de 2020 así como con el sufrido, entre otros, el 30 de octubre de 2020, cabe resaltar que:

[66] *Véase,* Operación Vóljov.

- El 28 de mayo de 2020 tuvo lugar la audiencia de extradición de Josu URRUTIKOETXEA BENGOETXEA, exdirigente de ETA y defendido de mi representado, en la que participó mi defendido; previa y posteriormente, se celebraron reuniones con los abogados franceses del Señor URRUTIKOETXEA BENGOETXEA.
- El 31 de mayo de 2020, mi representado participó en dos reuniones importantes celebradas por videoconferencia con el conjunto de la defensa de los líderes independentistas catalanes en el exilio, reunión en la que participaron otros abogados, asesores y los propios defendidos.
- El 2 de junio de 2020, mi representado participó en una reunión con Doña Laura BORRÁS, entonces diputada y actualmente Presidenta del Parlamento de Catalunya, y otra reunión celebrada por videoconferencia con los abogados de Bélgica y Alemania con los que lleva adelante la defensa de los políticos catalanes del *procés* exiliados en esos países.
- El 17 de junio de 2020, mi representado mantuvo entrevistas televisivas en diferentes medios de comunicación de

Catalunya y del País Vasco, así como también participó de un encuentro con el diputado Jon IÑARRITU.

- El 24 de junio, mi representado participó de reuniones presenciales con el expresidente Carles PUIGDEMONT, Toni COMIN, Clara PONSATÍ, Lluís PUIG, Josep Miguel ARENAS BELTRAN (Valtonyc) y los abogados de Bélgica con los que lleva adelante la defensa de los políticos catalanes exiliados, así como la del propio cantante Valtonyc.
- El 31 de octubre de 2020, mantuvo reuniones presenciales con diferentes clientes relevantes acerca de diversos casos penales y una reunión celebrada por videoconferencia con líderes independentistas catalanes en el exilio de cara a la revisión de diversos elementos esenciales en la defensa de sus intereses respecto del procedimiento de suplicatorio remitido por el Tribunal Supremo al Parlamento Europeo.

Los anteriores son solo algunos de los ejemplos de actuaciones profesionales afectadas por el espionaje sufrido por el Sr. BOYE y que, como se trata de casos y personas con relevancia pública, describirlos aquí no afecta al secreto profesional pero existen otros muchos, según la

agenda profesional del Sr. BOYE, que también se vieron afectados por este espionaje.

Por todo lo expresado, entendemos que existen sobrados elementos para iniciar una investigación con relación el espionaje practicado sobre el dispositivo móvil de mi representado mediante el software de inteligencia cibernética "Pegasus", producidos entre enero y mayo de 2020, así como también con respecto al sufrido a través de dicho programa espía sobre el dispositivo móvil de mi defendido, verificado al 30 de octubre de 2020 sin que se descarte que durante todo el periodo analizado el sistema de espionaje haya estado activado, que es algo que deberá determinarse en el curso de la presente investigación.

VI.- COMPETENCIA

En función de lo establecido por los artículos 14.2, 272 y concordantes de la Ley de Enjuiciamiento Criminal, resulta competente el Juzgado de Instrucción de Madrid que por turno corresponda al haberse cometido, al menos en parte, en ese partido judicial los hechos que se relacionan en este escrito.

En efecto, toda vez que el delito previsto en el art. 197.1 del Código Penal no se trataría de un delito de mera actividad sino de un delito de consumación anticipada[67], y por lo tanto bastaría con la interceptación de las comunicaciones para que el delito se consume, y en el caso que nos ocupa, la interceptación de aquéllas mediante la instalación del software malicioso de inteligencia cibernética "Pegasus" se produjo también en el dispositivo móvil del afectado mientras se encontraba en la ciudad de Madrid -sin perjuicio de una afectación más global producto de los múltiples desplazamientos del Sr. BOYE como consecuencia de sus obligaciones profesionales-, es posible concluir que, de acuerdo a la teoría del resultado, el lugar de producción del mismo habría sido allí y, por ende, resultaría este juzgado el competente para entender en la investigación de los hechos en cuestión.

VII.- FUNDAMENTOS DE DERECHO

VII.A.- INTRODUCCIÓN

[67] *SÁNCHEZ MELGAR, Julián; Código Penal. Comentarios y Jurisprudencia. Tomo I. 2004. Editorial Sepín, pág. 1096.*

Previo a exponer la significación jurídica de los sucesos denunciados, corresponde poner de manifiesto los argumentos en virtud de los cuales se infiere la ilegalidad del software de inteligencia cibernética "Pegasus".

El art. 18.3 de la Constitución Española garantiza el derecho al secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

Asimismo, el art. 12 de la Declaración Universal de los Derechos Humanos (10/12/1948) establece que:

> *"...nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques…".*

El art. 17 del Pacto Internacional de Derechos Civiles y Políticos (16/12/1976) indica que:

> *"...1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación…",*

y:

> *"...2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques…"*.

El art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (04/11/1950) prevé que:

> *"...1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia…"*,

y:

> *"...2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás…"*.

Los artículos mencionados deben ser tenidos en cuenta a la hora de interpretar los derechos fundamentales reconocidos en la Constitución Española, en función de lo que se prevé en el art. 10.2 de aquélla.

Por su parte, la Carta de los Derechos Fundamentales de la Unión Europea protege, en su

artículo 7, los mismos derechos cuando garantiza que:

> *"...Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones…"*,

y en su artículo 8, al establecer que:

> *"...1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*
>
> *3. El respeto de estas normas estará sujeto al control de una autoridad independiente..."*.

Derechos, todos estos, que han de ponerse en relación con otros de similar intensidad también protegidos en la mencionada Carta de los Derechos Fundamentales de la Unión Europea, norma de derecho primario, y que es de directa aplicación al caso que nos ocupa como se acreditará *ut infra*.

En cualquier caso, y a los efectos de normativa interna, la utilización del software malicioso de inteligencia cibernética "Pegasus" afecta de manera esencial al derecho fundamental

al secreto de las comunicaciones (art. 18.3 de la Constitución Española).

Además, y de acuerdo a lo expresado por el Tribunal Constitucional respecto a las intervenciones telefónicas -que podría estimarse una medida de limitación del derecho al secreto de las comunicaciones asimilable en cuanto a las consecuencias que produce la utilización del software de inteligencia cibernética "Pegasus", aunque de mucho menor entidad-, si bien:

> "*...el fundamento del carácter autónomo y separado del reconocimiento de este derecho fundamental* [derecho al secreto de las comunicaciones] *y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación…*",

lo cierto es que:

> "*...Este reconocimiento autónomo del derecho no impide naturalmente que pueda contribuir a la salvaguarda de otros derechos, libertades o bienes constitucionalmente protegidos, como el secreto del sufragio activo, la libertad de opinión, ideológica y de pensamiento, de la libertad de empresa, la confidencialidad de la asistencia letrada o,*

naturalmente también, el derecho a la intimidad personal y familiar…"[68].

No escapa a la consideración de esta parte que el derecho fundamental al cual viene haciéndose alusión en los párrafos que anteceden, al igual que otros derechos, no es absoluto. En efecto, en una sociedad democrática, y siempre bajo el respeto irrestricto del principio de legalidad, la necesidad de proteger valores esenciales como la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud, o la protección de los derechos y las libertades de los demás, pueden justificar la injerencia de la autoridad pública en el ejercicio de este derecho fundamental[69]. De hecho, el art. 18.3 de la Constitución española prevé la limitación del derecho al secreto de las comunicaciones mediante resolución judicial.

En este sentido, por la LECrim se establecen disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento,

---

[68] *Véase, STC 123/2002, del 20/05/2002, fundamento jurídico 5º.*
[69] *Véase, art. 8 del Convenio Europeo de Derechos Humanos.*

localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos[70], todas las cuales se vinculan con la regulación de medidas tecnológicas de investigación que, de acuerdo a las pautas allí establecidas, autorizan la limitación del derecho fundamental de que se trata en casos específicos.

De acuerdo a la normativa mencionada, la limitación al derecho fundamental al secreto de las comunicaciones no sólo requiere autorización previa mediante resolución judicial, sino que, además, aquella decisión debe encontrarse suficientemente motivada, dictada por un juez competente, en el marco de un procedimiento judicial de investigación de determinados delitos, con una finalidad específica que sustente la excepcionalidad, la temporalidad y la proporcionalidad de aquélla, y, además, **deberá ser ejecutada por funcionarios públicos españoles** y sometida a un estricto control judicial en su desarrollo y práctica[71]. En el caso de las intervenciones que sean solicitadas por el CNI no se da ese estricto control, sí en caso de prórroga, pero, de todas formas, dichas intervenciones han de ser materializadas por

[70] *Véase, arts. 588 bis a y ss. de la LECrim.*
[71] *Véase, arts. 588 bis.a, 588 bis.b, 588 bis.c, 588 bis.e, 588 bis.g, 588 bis.j, 588 bis.k, entre otros, de la LECrim.*

funcionarios españoles y no pueden serlo por empleados de una empresa extranjera.

Así, es pacífica la doctrina jurisprudencial establecida por el Tribunal Constitucional[72] y por el Tribunal Europeo de Derechos Humanos[73], de la cual se extrae que la restricción al derecho fundamental al secreto de las comunicaciones sólo puede considerarse constitucionalmente legítima si la medida restrictiva de aquel derecho se encuentra legalmente prevista con precisión -principio de legalidad-, autorizada por un órgano judicial en el marco de un proceso, con estricta observancia del principio de proporcionalidad, ejecutada bajo estrictos términos en cuanto a los límites materiales o temporales de la misma como a las condiciones de su autorización y sujeta a un control judicial efectivo.

Sin embargo, de acuerdo a la arquitectura y al modo de funcionamiento del software de inteligencia cibernética "Pegasus" -cuyas características principales fueron sucintamente descritas en el punto IV.II.A del presente-, se advierte que, **incluso en el caso hipotético de que la finalidad de su utilización se encuentre**

---

[72] *Véase, SSTC 114/1984, 5/1994, 86/1995, 181/1985, 49/1996, 54/1996, 81/1998, 121/1998, 151/1998 y 49/1999.*

[73] *Véase, STEDH en casos: "Klass" -de fecha 6 de septiembre de 1978-, "Malone" -de fecha 2 de agosto de 1984-, "Kruslin y Huvig" -de fecha 24 de abril de 1990-, "Halford" -de fecha 25 de marzo de 1998-, "Klopp" -de fecha 25 de marzo de 1998- y "Valenzuela" -de fecha 30 de julio de 1998-.*

sustentada en motivos legales -los cuales, como se verá, tampoco se aprecian en el presente caso -, **aquél no resulta compatible con los principios rectores y presupuestos esenciales establecidos por la legislación y por la jurisprudencia para habilitar la limitación del ejercicio del derecho fundamental al secreto de las comunicaciones mediante medidas de investigación tecnológica.**

En apoyo de lo aquí afirmado, cabe expresar que si se tiene en consideración que el software de inteligencia "Pegasus", una vez instalado en el dispositivo móvil de que se trate, concede acceso ilimitado a toda la información del mismo, inclusive lo datos más sensibles e íntimos de una persona, difícilmente una medida de investigación tecnológica de este calibre cumple con el principio de proporcionalidad[74].

Con relación a este punto, el Supervisor Europeo de Protección de Datos, Wojciech Wiewiórowski -oportunamente designado por el Parlamento y el Consejo de la Unión Europea[75]-, ha indicado recientemente que el nivel de interferencia con el derecho a la privacidad -en referencia a la utilización del software de inteligencia cibernética "Pegasus"- es tan severo

[74] *Véase, art. 588 bis a de la LECrim y el art. 52 de la Carta de Derechos Humanos de la Unión Europea.*
[75] *The Supervisor.*

que el individuo objeto del mismo es de hecho privado del mismo[76].

El Supervisor Europeo de Protección de Datos hace hincapié en que, independientemente de que el software de que se trata pueda considerarse necesario para alcanzar los objetivos de un estado democrático -que no es lo que ocurre en este caso-, lo cierto es que ello no implica que sea proporcional, máxime si se tiene en cuenta que no sólo la persona que es objeto del ataque mediante esta herramienta es absolutamente privada de su derecho al secreto a las comunicaciones y de su intimidad, sino que, además, de acuerdo a las enormes capacidades tecnológicas del software en cuestión, quienes hayan estado en contacto o alrededor de aquélla también le son infringidos estos derechos. A título de ejemplo de la incompatibilidad de esta herramienta tecnológica con el principio de proporcionalidad, el Supervisor Europeo de Derechos Humanos indica que la utilización de "Pegasus" puede generar situaciones en las cuales inclusive las personas que casualmente se encuentran sentadas en un restaurante cercanas al objetivo también puedan ser grabadas en sus conversaciones privadas mediante una activación remota del micrófono y/o cámara del dispositivo telefónico espiado.

[76]. *EDPS Preliminary Remarks on Modern Spyware | European Data Protection Supervisor*.

En el mismo sentido, el ilimitado acceso y recopilación en tiempo real de todas las comunicaciones del objetivo, en ocasiones en las que aquél se encuentre reunido, por ejemplo, con un abogado como ha ocurrido en el presente caso, también puede implicar una vulneración del secreto profesional[77] y cuando el objetivo es un abogado -o reuniones abogado-cliente como ocurren en varios de los actos aquí descritos- el secreto profesional al que se debe, así como el de todos sus defendidos y los demás abogados con los que se relacione quedarán irremediablemente afectados.

En cuanto se vincula específicamente con el secreto profesional de las relaciones abogado-cliente, no puede perderse de vista, en referencia al principio de proporcionalidad al que se hizo alusión por los párrafos anteriores, que el Tribunal Europeo de Derechos Humanos ha establecido que cuando se encuentra en juego esta garantía la limitación de la misma debe estar sometida a un control de proporcionalidad, incluso, mucho más riguroso[78], lo que no hace más que dar sustento mayor a la incompatibilidad de la utilización de "Pegasus" con aquel principio y, por ende, su ilegalidad, cuando el afectado

---

[77] *Véase, art. 5 del Código Deontológico de la Abogacía Española, arts. 22 y 23 del Estatuto General de la Abogacía Española y art. 199 del Código Penal.*

[78] *Véase, STEDH dictada en el caso "Goodwin c. Reino Unido", de fecha 27 de marzo de 1996.*

por el software de ciberinteligencia mencionado se trata de un abogado y/o sus clientes.

En línea con lo expresado con respecto al secreto profesional, en el caso que nos ocupa, y siempre haciendo referencia al hipotético caso de que este software de inteligencia cibernética fuese utilizado en base a motivos legales (que no es el caso) -a título de ejemplo, en el marco de una investigación judicial[79]-, dada la potencialidad que tiene el mismo de extraer, prácticamente, toda la información contenida en un dispositivo móvil, implicaría que las autoridades accedan, indefectiblemente, a información ajena incluso a los hechos objeto de investigación -como lo es la relativa a la confidencialidad de la relación abogado-cliente-, cuestión que, de acuerdo a la doctrina establecida por el Tribunal Europeo de Derechos Humanos, en el caso de los abogados, redunda en una grave violación al derecho a la intimidad y al secreto profesional[80].

Otro tanto ocurre en el caso del secreto profesional de los periodistas; debe tenerse presente dos variantes en el presente caso: a) que hay periodistas espiados, y b) que la casi totalidad de los afectados son personas con

[79] Lo que no sucedería en el supuesto de los hechos que se denunciarán por esta presentación.

[80] *Véase, en este sentido, STEDH dictada en el caso "Sargava c. Estonia", de fecha 16 de noviembre de 2021.*

proyección pública que mantienen constante contacto con periodistas. En uno y otro caso se ha afectado el secreto profesional de los periodistas, tanto por ser afectados como objetivos como por ser una suerte de "daño colateral".

En este sentido, el Tribunal Constitucional ha reconocido a los profesionales del derecho a la cláusula de conciencia y al secreto profesional para asegurar el modo de ejercicio de su fundamental libertad de información[81].

Por otra parte, como ya fue señalado por el punto IV.II.A, pese a que "N.S.O. GROUP" publicita un detalle pormenorizado de la arquitectura y funcionalidades del software de inteligencia cibernética de que se trata, resulta llamativo el hecho de que aquella compañía no especifique en qué servidores es alojada la información extraída de los dispositivos móviles o sistemas de información atacados ni por quién es administrada ni por cuánto tiempo es conservada y, ni mucho menos, si luego de su utilización es destruida o no.

Lo que se ha logrado determinar es que esta omisión esconde la irregularidad relativa a que **todo el proceso de espionaje es materializado**

[81] *Véase, STC 225/02, de fecha 9 de diciembre de 2002.*

por los empleados de la propia empresa "N.S.O. GROUP" y los datos obtenidos son almacenados en sus servidores con lo que ni es llevado a cabo por funcionarios públicos españoles ni los datos extraídos son mantenidos en un servidor de los cuerpos y fuerzas de seguridad española o de la Central Nacional de Inteligencia sino en los de una empresa privada en el extranjero, por lo que quien realiza el encargo de espionaje solo recibe una copia de lo obtenido pero nunca el original del material espiado.

En este sentido, resulta relevante poner de relieve lo manifestado recientemente por Bill MARCZAK[82] en la audiencia pública organizada por el Partido Popular Europeo que tuvo lugar el pasado 10/02/2022 en el Parlamento Europeo[83]. A saber, el nombrado indicó:

> *"…La gran pregunta acerca de "Pegasus", es ¿Quién es exactamente el que tiene acceso a la información que es extraída de los dispositivos móviles mediante este software? Lo que nosotros concluimos es que hay una suerte de entidad centralizada, probablemente "N.S.O. GROUP", que establece servidores para todos los diferentes clientes de la compañía, y la información que es extraída de los dispositivos móviles atacados fluye a través de estos servidores, pero la pregunta es: ¿Hacia dónde exactamente va esa*

[82] *Investigador Senior en Citizen Lab, co-fundador de Bahrain Watch y PhD en Ciencias de la Computación (UC Berkeley).*
[83] *Véase, a estos efectos, el vídeo del evento:LIVE: Pegasus spyware scandal and its impact on democracy in the EU*

información? Claramente, esa información llega a los clientes de "Pegasus" que iniciaron el monitoreo de los dispositivos móviles atacados bajo el software de que se trata, pero también esa información podría estar siendo enviada a algún otro lugar. Lo que vimos es que la revelación del escándalo de "Pegasus" en Israel no sólo reveló el indebido uso de "Pegasus" por parte de la policía local, sino también implicó revelaciones acerca de cómo N.S.O. opera como compañía, en tanto se habría revelado el hecho de que el CEO de N.S.O. habría tenido reuniones diarias o muy frecuentes con el Ministro de Defensa de Israel. También vimos casos, de hecho, un caso en el que yo trabajé, en el cual N.S.O. tomó el extremo e inusual paso de notificar a un objetivo de vigilancia mediante "Pegasus" por mucho tiempo acerca de que se había estado realizando vigilancia sobre su dispositivo, pero lo llamativo es que justo realizaron esa notificación apenas después de que yo había notificado personalmente al objetivo de esa situación. Ante esta circunstancia, N.S.O. alegó que 'recibieron una información que derivó en la notificación', pero ¿de quién?, no lo dijeron, pero lo cierto es que si alguien no estaba mirando, entonces ¿cómo lo supieron?...".

Asimismo, el investigador de CITIZEN LAB agregó:

"...El rol de "Pegasus" va mucho más allá que simplemente crear el producto, venderlo y lavarse las manos. Una herramienta como "Pegasus" es prácticamente inútil sin actualizaciones

constantes, mantenimiento y ayuda de parte de N.S.O...".

Y, en este sentido, agregó que:

> *"...Me parece que es importante, en el contexto de cualquier investigación o de un potencial esfuerzo de establecer regulaciones sobre este tema, tener en cuenta que esta tecnología es prácticamente inútil sin el servicio continuo de la compañía que lo administra, y las investigaciones o las regulaciones deberían poner el foco en revelar aún más el rol de estas compañías en vez de centralizarse más en la tecnología en sí misma...".*

De acuerdo a las circunstancias puestas de manifiesto *ut supra*, en primer lugar, cabe expresar que la indudable intervención que "N.S.O. GROUP" tiene en el proceso de recopilación de información del dispositivo móvil atacado, así como de su posterior administración y guarda, resulta incompatible con el presupuesto legal relativo a que la medida de investigación tecnológica sólo puede estar a cargo de funcionarios públicos (Policía Judicial)[84].

Esta incompatibilidad también sería trasladable al hipotético caso de que haya sido el Centro Nacional de Inteligencia el que, en el marco del desarrollo de sus actividades, hubiere utilizado "Pegasus" en una investigación de

[84] *Véase, art. 588 bis.b.5° de la LECrim.*

seguridad en los términos de la normativa reguladora de aquel centro[85].

Esto es así pues, si bien el Centro Nacional de Inteligencia puede desarrollar actividades que impliquen restricciones de derechos fundamentales -como las que afectan al del secreto a las comunicaciones- mediante autorización del Tribunal Supremo[86], lo cierto es que aquellas actividades deben ser al amparo del principio de legalidad y en este contexto, si se tiene en consideración el modo en que se recopila, se administra y se conserva la información obtenida mediante el programa espía "Pegasus", tareas que son ejecutadas en esencia, como se expresó anteriormente, por empleados de "N.S.O. GROUP" y en servidores de esa misma empresa, la utilización de este software de inteligencia cibernética por parte del Centro Nacional de Inteligencia resulta incompatible con la exigencia legal a la cual se hizo alusión *ut supra*, la que en el caso de este organismo debe ser aplicable supletoriamente.

Asimismo, y desde otra perspectiva, la intervención de "N.S.O. GROUP" en el proceso de recopilación, administración y conservación de datos obtenidos mediante la utilización de este software de inteligencia cibernética, vulnera o

[85] *Véase, LO 11/2002, del 6 de mayo de ese año.*
[86] *Véase, Disposición adicional única, punto 4°, que añade como art. 342 bis a la LO 6/1985, del 1 de julio, del Poder Judicial.*

pone en peligro excesivo el secreto que aquella medida debe guardar más allá de las partes intervinientes[87] -dando por sentada que dicha herramienta sea utilizada en el marco de un procedimiento judicial; que en el presente caso también cabe poner en duda-, así como también el principio de temporalidad que debe imperar en aquélla[88], y la posibilidad de efectuar un control judicial efectivo sobre la misma[89].

Dicho más claramente: incluso si quien hubiese practicado este espionaje hubiese sido el Centro Nacional de Inteligencia dicha medida habría tenido que ser, de una parte, autorizada por el Juez encargado en el Tribunal Supremo -basándose, entre otras cosas en el principio de proporcionalidad y de necesidad que no se dan en este caso- y las intervenciones deberían haberse practicado por funcionarios públicos españoles, cosa que tampoco se da en el caso de hacerse a través del sistema "Pegasus".

En esta misma línea, y quizás una de las circunstancias que puede traer aparejada una vulneración indeterminada en el tiempo del derecho al secreto de las comunicaciones de la persona que es sometida a este software de inteligencia cibernética, es que, al no poder determinar y controlar quiénes terminan teniendo

[87] *Véase, art. 588 bis.d de la LECrim.*
[88] *Véase, art. 588 bis.e de la LECrim.*
[89] *Véase, art. 588 bis.g de la LECrim.*

acceso a la información extraída del dispositivo atacado, así como también con respecto a los servidores donde es almacenada aquélla para su conservación -primigeniamente en los de las empresas querelladas, tampoco resulta posible garantizar y, por ende, cumplir, con la obligación legal relativa al borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, una vez que se ponga término al procedimiento judicial de que se trate.

Por último, y como una circunstancia que justifica aún más la evidente ilegalidad de un software de inteligencia cibernética como "Pegasus", cabe expresar que, tal como surge del reciente informe emitido por The Citizen Lab con relación a la amplia utilización de este software espía contra diversos políticos catalanes, periodistas y abogados en España, entre otras personas[90], se ha logrado determinar que, entre las capacidades de "Pegasus", **se encuentra la de modificar el sistema operativo y los archivos de un dispositivo infectado**. A título de ejemplo, enaquel informe se hace mención a la capacidad del software de enviar mensajes bajo la identidad de la víctima.

[90] *Véase, informe completo y gráfico "Catalan Gate".*

Esto significa que quien realiza el ataque mediante este software espía no sólo tiene la posibilidad de tener acceso ilimitado a toda la información de un sistema de información, inclusive lo datos más sensibles e íntimos de una persona, y de extraer de forma remota y secreta del mismo esa información y transmitirla para su análisis a un servidor en el que aquélla es alojada para ser reproducida en cuanto sea necesario -con las incompatibilidades legales y la violación de derechos fundamentales que ello implica, las que fueron sucintamente descritas a lo largo de este punto-, sino que, como si esto no fuera poco, también tiene la posibilidad de vulnerar la integridad de esa información, modificándola o contaminándola a su antojo mediante la introducción, incluso, de archivos o datos que nunca estuvieron en dicho dispositivo.

Esta circunstancia, eleva de un modo desmedido el riesgo de que este software espía sea utilizado indebidamente por quienes realizan el ataque a los fines de contaminar y/o "plantar" pruebas en los teléfonos atacados, todo lo cual, no sólo atenta a la integridad de esos datos -que desde ya representa un perjuicio para el titular de los mismos-, sino contra el valor probatorio de aquéllos en el contexto de investigaciones y/o enjuiciamientos penales.

En estas condiciones, va de suyo que la utilización de "Pegasus" invalida cualquier investigación judicial contra una persona que haya sido objeto de ataques de este software espía en sus dispositivos electrónicos, pues no podría asegurarse con certeza la integridad de la evidencia que se extraiga de aquéllos, y por ende, la investigación correría la misma suerte.

En función de lo aquí argumentado, resulta posible concluir que, de acuerdo a los presupuestos legales y principios rectores que regulan las medidas de investigación tecnológica, el software de inteligencia cibernética "Pegasus" resulta manifiestamente ilegal, independientemente de si los motivos de su utilización resulten compatibles con la protección de valores esenciales de una sociedad democrática o no.

Sin embargo, como se desarrollará en el apartado siguiente, incluso en el caso hipotético de considerar a este software de inteligencia cibernética como una herramienta legal en abstracto -que no lo es-, su utilización en los sucesos que aquí se denuncian, demostrarán justamente todo lo contrario.

VII.B.- CALIFICACIÓN JURÍDICA DE LOS HECHOS

Sin perjuicio de una posterior y más acertada calificación jurídica de los hechos denunciados por esta representación y de la concreción de la participación en ellos de los querellados y de todos los que eventualmente resulten responsables por los mismos, ya desde este momento inicial, aquéllos revisten los caracteres del delito previsto y penado en el 197.1 del Código Penal, y en el art. 197 bis.1 del mismo cuerpo legal, con la circunstancia agravante prevista en el art. 197 quater del mismo código.

Por el art. 197.1 del Código Penal, se prevé:

> *"El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".*

De acuerdo a lo establecido por la jurisprudencia, el tipo penal transcrito en el párrafo que antecede protege el bien jurídico de la intimidad personal (art. 18.1 de la

Constitución española)[91], y en un sentido más específico, la doctrina ha delimitado el campo de su protección desde la perspectiva del derecho al secreto de las comunicaciones -en especial, las postales, las telegráficas y las telefónicas-, salvo resolución judicial (art. 18.3 de la Constitución española)[92].

En cuanto se relaciona con los presupuestos que deben ser tenidos en cuenta para tener por configurado el tipo penal de que se trata, cabe expresar que aquél requiere por parte del sujeto activo una conducta de apoderamiento, de interceptación o de utilización de artificios técnicos -elemento objetivo- que se encuentre conectada con la intención o ánimo del mismo de descubrir un secreto o vulnerar la intimidad de otro -elemento subjetivo-, sin que resulte necesario a los efectos de la consumación del delito en cuestión la producción del descubrimiento del secreto o la vulneración de la intimidad.

En este sentido, el Tribunal Supremo ha establecido que:

> "...[el tipo penal de que se trata] *es una figura delictiva que se integra en la categoría*

---

[91] *Véase, entre otras, STS 694/03, de fecha 20 de junio de 2003 ; STS 237/07, de fecha 21 de marzo de 2007.*

[92] *Véase BARREIRO, Agustín Jorge; El delito de descubrimiento y revelación de secretos en el código penal de 1995: un análisis del artículo 197 del CP. Revista Jurídica Universidad Autónoma De Madrid, (6).*

de los delitos de intención, y en la modalidad de delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional al dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse. Por ello, la conducta típica del artículo 197.1, se consuma con el apoderamiento, interceptación, etc., sin necesidad que se produzca el efectivo descubrimiento de los secretos, o vulneración de la intimidad, siendo posibles las formas imperfectas de ejecución, tentativa acabada o inacabada…"[93].

En cuanto a la significación jurídica del del verbo típico "se apodere", si bien por la doctrina se ha indicado que aquél debe entenderse desde la concepción jurídica otorgada al "apoderamiento patrimonial", esto quiere decir, traducido a la materia de que se trata, que debe exigirse para la consumación del delito una traslación del objeto a manos del sujeto activo que implique la aprehensión física del soporte en el que se encuentren los datos, quedando por fuera del tipo penal la simple captación mental del secreto[94], lo cierto es que, con el avance de la tecnología, no puede perderse de vista que la

---

[93] Véase, STS 694/03, de fecha 20 de junio de 2003; y en el mismo sentido, STS 358/07, de fecha 30 de abril de 2007, y STS 379/18, de fecha 23 de julio de 2018.

[94] Véase ANARTE BORRALLO, E., Consideraciones sobre los delitos de descubrimiento de secretos. En especial, el artículo 197.1 del código penal. Jueces para la Democracia, Nº 43, 2002.

aprehensión física no es la única forma de "desapoderar" a una persona de un secreto o de cualquier otra vulneración de su intimidad, en el sentido que expresa el tipo penal.

En esta línea argumental, el Tribunal Supremo ha establecido que:

> *"...El apoderamiento de documentos exigido en el art. 197 CP, por tanto,* ***no puede considerarse estrictamente como el apoderamiento físico de los mismos. Basta con su aprehensión virtual, de manera que el sujeto activo del delito se haga con su contenido de cualquier forma técnica que permita su reproducción posterior****…"*[95].

Por otra parte, y en lo que respecta a lo que debe entenderse jurídicamente como "interceptar las telecomunicaciones", se ha indicado que aquella conducta se refiere a la acción del sujeto activo mediante la cual le permita al mismo introducirse en una conversación ajena con el ánimo de descubrir los secretos de otro o de vulnerar su intimidad[96], y en este sentido es pacífica la doctrina y la jurisprudencia en cuanto a que las telecomunicaciones a las que se refiere el tipo penal analizado no sólo comprenden las comunicaciones telefónicas tradicionales o por

---

[95] *Véase STS 538/21, de fecha 17 de junio de 2021.*

[96] *Véase, LORAZNO MIRALLES, J.; en VV.AA., Compendio, P.E., II, pág. 212, y SEGRELLES DE ARENZA, I; en VV.AA, Compendio, P.E., pág. 278.*

cable, sino también las que tienen lugar mediante **telefonía móvil, sin que resulte relevante el sistema que utilicen los interlocutores**[97].

A su vez, y en cuanto a la concepción que debe otorgarse a la conducta de "utilizar artificios técnicos", debe entenderse como una acción del sujeto activo mediante la cual, empleando esa clase de medios, se grabe un sonido o se capte una imagen con la intención de descubrir un secreto o vulnerar la intimidad de otro, resultando atípicas las conductas que, aunque en abstracto puedan implicar una vulneración de la intimidad en sentido amplio, se lleven a cabo sin esos artificios, como puede ser escuchar una conversación detrás de una puerta.

Finalmente, y previo a exponer las razones por las cuales los sucesos denunciados encontrarían significación jurídica desde la perspectiva del tipo penal al cual viene haciéndose alusión, corresponde efectuar algunas consideraciones acerca de qué debe entenderse por secreto o vulneración de la intimidad.

---

[97] *Véase QUERALT JIMÉNEZ, J.J.; Derecho Penal, P.E. Atelier. 2010; CARMONA SALGADO, C; La intimidad como bien jurídico protegido, a propósito de la reforma penal sobre secreto de las comunicaciones, de 23 de diciembre de 1994, en VV.AA., Comentarios a la legislación penal, XVII, dir. M. COBO y coord. M. BAJO, 1996; Auto de la Audiencia Provincial de Madrid (Sección 15) del 10 de mayo de 1996; SAP de Madrid (Sección 15) del 26 de mayo de 1999; y STC 34/1996, de fecha 17 de abril de 1996.*

Con relación a este punto, por la doctrina se ha establecido un concepto jurídico amplio de secreto, el que no se refiere únicamente a lo oculto y reservado, sino, más bien, a todo conocimiento reservado que el sujeto activo no conozca, o no esté seguro de conocer, y que el sujeto pasivo no quiera que conozca[98].

En sentido similar, el Tribunal Supremo ha expresado que:

> *"...En la STS 666/2006, de 19 de junio, se dice que 'la idea de secreto en el art. 197,1º Cpenal resulta conceptualmente indisociable de la de intimidad' que es, a su vez, 'ese ámbito propio y reservado frente a la acción y el conocimiento de los demás' (SSTC 73/1982 y 57/1994, entre muchas). En este sentido, se ha dicho, y es universalmente aceptado, que el de intimidad es un concepto psicológico que remite a ese 'mundo propio' en el que cada quien desarrolla su 'vida interior'. Por tanto, un reducto que está más allá de la privacidad y que conecta con los estratos más profundos de la personalidad, de la que es primera manifestación.*
>
> *Así las cosas, no hay duda, todo lo situado dentro de esa esfera tiene especial relevancia para el sujeto, en tanto que lo constituye como tal, y contribuye de manera decisiva a distinguirle. Esto no excluye que puedan darse*

---

[98] *Véase VIVES ANTÓN, T. S., BOIX REIG, J., ORTS BERENGUER, E., DEL ROSAL BLASCO, B, MARTÍNEZ BUJÁN PÉREZ, C., MONTÉS PENADÉS, V. L., CARBONELL MATEU, J. C., GONZÁLEZ CUSSAC, J. L.,SÁNCHEZ YLLERA, I., GUINARTE, G.; Comentarios al código penal de 1995. Tirant lo blanch. 1996.*

grados de intensidad en la pertenencia o inherencia a ese espacio, de los concretos asuntos o actitudes que son propios del mismo. Y ello, por razón de su calidad específica y de la valoración que merezcan en el plano ético o de la autoestima al sujeto mismo; o incluso de la que este entienda que, de ser conocidos, pudieran obtener en el entorno, a tenor de los estándares de moral social imperantes. Pero en cualquier caso, no hay duda, en rigor, lo íntimo estará siempre integrado por o tendrá que ver con el conjunto de vivencias, experiencias o rasgos caracteriales exclusivos que el individuo, como regla, aspira a mantener bajo reserva y para sí, al tratarse de datos que le comprometen de manera intensa, porque son de los que le hacen ser, precisamente, el que es como persona. Tanto es así, que en el lenguaje coloquial, cuando alguien invade de alguna forma y conoce lo que de otro se oculta en esa dimensión particularísima, se dice, bien expresivamente, que 'lo tiene en sus manos'.

La intimidad es, por eso, contenido de un derecho fundamental, que goza de la protección del art. 18 de la Constitución. En este figura asimismo el secreto como derecho igualmente fundamental, que también comparte con aquélla el tipo penal a examen. Ahora bien, esta contigüidad en el orden de la garantía normativa no puede hacer perder de vista la diversidad conceptual, que se proyecta también en este mismo plano. En efecto, pues el de intimidad es un concepto, ético-psíquico y, por eso, cabe decir, material o sustantivo ; mientras el de secreto es un artificio jurídico-formal , puesto

constitucionalmente al servicio de una diversidad de bienes jurídicos, y aquí, concretamente, de la primera, para tratar de preservarla o asegurarla cuando, por salir de su espacio original y entrar en el de la comunicación, resulta más vulnerable y debe ser más intensamente protegida. En este sentido y, en rigor, el término 'secretos' yuxtapuesto al de 'intimidad' en el art. 197,1º Cpenal, podría decirse que no añade nada a la segunda , o nada realmente significativo en el plano de los contenidos..."[99].

De lo expresado en el art. 197.1 del Código Penal, esta parte entiende que, en el caso que nos ocupa, concurren perfectamente los presupuestos establecidos por la doctrina y por la jurisprudencia para estimar fundadamente que mi representado ha sido víctima del delito de descubrimiento de secretos previsto y penado por la norma aludida precedentemente.

En efecto, de acuerdo a la arquitectura y al modo de funcionamiento del software de inteligencia cibernética "Pegasus" -**cuyas características principales fueron sucintamente descritas por el punto IV.II.A del presente**-, la efectiva instalación y utilización del software de mención en el dispositivo de mi defendido no sólo implicó un apoderamiento de sus secretos documentales, sino, también, la interceptación de sus telecomunicaciones y la utilización de

[99] *Véase STS 534/11, de fecha 10 de junio de 2011.*

artificios técnicos de grabación de sonido y captación de la imagen, todo ello con el propósito de vulnerar gravemente su intimidad así como, especialmente, **su secreto profesional como abogado en ejercicio que es y que, además, defiende a un número significativo de afectados por el espionaje masivo practicado mediante el uso de la aplicación "Pegasus" como se ha expuesto *ut supra*.**

En cuanto se relaciona con la vulneración del secreto profesional que se verifica en el caso por la condición de abogado en ejercicio de mi representado, y como una cabal demostración de cómo esa vulneración se traduce en la violación de la relación de confidencialidad del Sr. BOYE con sus defendidos, y por extensión, también en una vulneración de los derechos fundamentales de estos últimos -como el derecho de defensa, entre otros-, el Tribunal Supremo ha expresado:

> *"...la confidencialidad de las relaciones entre el imputado y su letrado defensor, que naturalmente habrán de estar presididas por la confianza, resulta un elemento esencial (STEDH Castravet contra Moldavia, de 13 de marzo de 2007, p. 49; y STEDH Foxley contra Reino Unido, de 20 de junio de 2000, p. 43). En la STEDH de 5 de octubre de 2006, caso Viola contra Italia, se decía que '...el derecho, para el acusado, de comunicar con su abogado sin ser oído por terceras personas figura entre las exigencias*

elementales del proceso equitativo en una sociedad democrática y deriva del artículo 6.3 c) del Convenio. Si un abogado no pudiese entrevistarse con su cliente sin tal vigilancia y recibir de él instrucciones confidenciales, su asistencia perdería mucha de su utilidad (Sentencia S. contra Suiza de 2 de noviembre 1991, serie A núm. 220, pg. 16, ap. 48). ***La importancia de la confidencialidad de las entrevistas entre el acusado y sus abogados para los derechos de la defensa ha sido afirmada en varios textos internacionales, incluidos los textos europeos*** *(Sentencia Brenan contra Reino Unido, núm. 39846/1998, aps. 38-40, TEDH 2001-X)'.*

En este mismo sentido, el Tribunal de Justicia de las Comunidades Europeas en la Sentencia (Gran Sala) de 14 de setiembre de 2010, señaló que 'la confidencialidad de las comunicaciones entre los abogados y sus clientes debía ser objeto de protección a nivel comunitario', aunque supeditó tal beneficio a dos requisitos: '...por una parte, debe tratarse de correspondencia vinculada al ejercicio de los derechos de la defensa del cliente, y, por otra parte, debe tratarse de abogados independientes, es decir, no vinculados a su cliente mediante una relación laboral'.

En el desarrollo de la comunicación entre letrado y cliente, basada en la confianza y en la seguridad de la confidencialidad, y con mayor razón en el ámbito penal, es lo natural que aparezcan valoraciones sobre lo sucedido según la

versión del imputado, sobre la imputación, sobre las pruebas existentes y las que podrían contrarrestar su significado inculpatorio, sobre estrategias de defensa, e incluso podría producirse una confesión o reconocimiento del imputado respecto de la realidad de su participación, u otros datos relacionados con la misma. Es fácil entender que, si los responsables de la investigación conocen o pueden conocer el contenido de estas conversaciones, la defensa pierde la mayor parte de su posible eficacia. En la primera de las sentencias antes citadas, Castravet contra Moldavia, el TEDH afirmó en este sentido que '...si un abogado no fuera capaz de departir con su cliente y recibir instrucciones de él sin supervisión, su asistencia perdería gran parte de su utilidad, teniendo en cuenta que el Convenio pretende garantizar derechos prácticos y efectivos'.

No es preciso, por lo tanto, que aparezca un aprovechamiento expreso mediante una acción concreta y directamente relacionada con lo indebidamente sabido, pues basta para lesionar el derecho de defensa con la ventaja que supone para el investigador la posibilidad de saber, *(y con mayor razón el conocimiento efectivo), si el imputado ha participado o no en el hecho del que se le acusa, saber si una línea de investigación es acertada o resulta poco útil, saber cuál es la estrategia defensiva, cuales son las pruebas contrarias a las de cargo, o incluso conocer las impresiones, las necesidades o las preocupaciones del imputado, o los consejos y sugerencias que le hace su letrado defensor. Se trata de*

aprovechamientos más sutiles, pero no por eso inexistentes. Basta, pues, con la escucha, ya que desde ese momento se violenta la confidencialidad, elemento esencial de la defensa. El TEDH ha señalado en este sentido que la injerencia existe desde la interceptación de las comunicaciones, sin que importe la posterior utilización de las grabaciones (STEDH Kopp contra Suiza, de 25 de marzo de 1998).

Además, sufrirían reducciones muy sustanciales otros derechos relacionados. En primer lugar, el derecho a no declarar. La comunicación con el letrado defensor se desarrolla en la creencia de que está protegida por la confidencialidad, de manera que en ese marco es posible que el imputado, solo con finalidad de orientar su defensa, traslade al letrado aspectos de su conducta, hasta llegar incluso al reconocimiento del hecho, que puedan resultar relevantes en relación con la investigación. Es claro que el conocimiento de tales aspectos supone la obtención indebida de información inculpatoria por encima del derecho a guardar silencio. En estos casos, la prohibición de valoración de lo ya conocido no es más que un remedio parcial para aquellos casos en los que, justificada la intervención con otros fines, el acceso haya sido accidental e inevitable, pero de esa forma no se elimina la lesión ya causada en la integridad del derecho.

En segundo lugar, el derecho al secreto profesional. Concebido como un derecho del letrado a no revelar los datos, de la clase que

sean, proporcionados por su cliente, o, con carácter más general, obtenidos en el ejercicio del derecho de defensa (artículo 416 de la LECrim y 542.3 de la LOPJ), opera también como un derecho del imputado a que su letrado no los revele a terceros, ni siquiera bajo presión. El conocimiento indebido del contenido de las comunicaciones entre ambos, pues, dejaría en nada este derecho.

En tercer lugar, el derecho a la intimidad. La relación entre el imputado y su letrado defensor se basa en la confianza, de forma que es altamente probable que estando el primero privado de libertad traslade al segundo cuestiones, observaciones o preocupaciones que excedan del derecho de defensa para residenciarse más correctamente en el ámbito de la privacidad, que solo puede ser invadido por el poder público con una razón suficiente.

No se trata, por otra parte, de derechos absolutos. El TEDH, en la Sentencia Viola contra Italia, de 5 de octubre de 2006 , señaló que '...el acceso de un acusado a su abogado puede estar sometido a restricciones por razones válidas. Se trata de saber en cada caso si, a la luz del conjunto del procedimiento, la restricción privó al acusado de un proceso equitativo'.

Pero sus posibles restricciones, que no siempre son aceptables en la misma medida, requieren, según la interpretación que el TC ha hecho de la Constitución y el TEDH del Convenio, del cumplimiento suficiente de, al menos, tres

exigencias. En primer lugar, una previsión legal suficiente, (en este sentido, STC 196/1987 y otras muchas), que en nuestro ordenamiento, en tanto que ley de desarrollo de un derecho fundamental, debe respetar en todo caso su contenido esencial (artículo 53.1 CE). En segundo lugar, una justificación suficiente en el supuesto concreto, que tenga en cuenta los indicios disponibles en el caso, la necesidad de la medida y el respeto al principio de proporcionalidad. A este aspecto se refieren la STEDH de 2 noviembre 1991 Caso S. contra Suiza y la STEDH de 31 enero 2002 Lanz contra Austria. Y en tercer lugar, en nuestro Derecho, una autorización judicial, regulada en ocasiones de forma expresa y en otras de forma implícita, según ha establecido el TC, aunque su forma y características admitan algunas matizaciones en función de la entidad de la restricción.

Naturalmente, todas estas consideraciones no pueden entenderse referidas solo a los efectos que producen en el caso concreto las escuchas de las comunicaciones reservadas entre el imputado y su letrado defensor. ***De aceptarse que la mera posibilidad de que se sigan cometiendo delitos justifica la supresión de la confidencialidad entre el imputado preso y su letrado defensor, desaparecería de manera general un elemento esencial en la misma configuración del proceso justo.*** *Incluso la mera sospecha fundada acerca de la existencia de escuchas generalizadas de las comunicaciones entre el imputado privado de libertad y su letrado defensor, anularía de manera general la confianza en una defensa con*

capacidad de efectividad, como elemento imprescindible para un proceso con igualdad de armas; un proceso, por tanto, equitativo. En este sentido, en la STEDH Castravet contra Moldavia, de 13 de marzo de 2007 , antes citada, ya se advirtió que '...una injerencia en el privilegio abogado-cliente, y por ende, en el derecho del detenido a la defensa, no exige necesariamente que tenga lugar una intercepción real o una escucha subrepticia. Una creencia genuina, basada en indicios razonables de que su conversación está siendo escuchada, puede ser suficiente, desde el punto de vista del Tribunal, para limitar la efectividad de la asistencia que el abogado pueda proporcionar. Tal creencia inhibiría inevitablemente la libertad de discusión entre el abogado y el cliente, y vulneraría el derecho del detenido a rebatir de forma efectiva la legalidad de su detención'..."[100].

No puede perderse de vista que, a diferencia del supuesto de hecho en el marco del cual el Tribunal Supremo expresó los fundamentos transcritos precedentemente, en el presente caso, **ni siquiera se advierte que haya existido una previsión legal suficiente que sustente la utilización de un programa espía como "Pegasus"** -que como se argumentó *ut supra* se infiere ilegal-, **ni una justificación suficiente en los términos de la necesidad y proporcionalidad de la medida** -que como también se fundamentó, no se

[100] *Véase, STS 79/2012, del 9 de febrero.*

cumple-, ni mucho menos una autorización judicial que haya permitido la utilización de una medida restricción del derecho al secreto de las comunicaciones de este calibre sobre mi defendido y de forma masiva sobre miembros de la minoría nacional catalana.

Siguiendo con la argumentación acerca de la verificación en el caso de los presupuestos del delito penado y previsto en el art. 197.1 del Código Penal, concretamente el apoderamiento de secretos documentales, si se tiene en cuenta que, una vez que "Pegasus" se encuentra correctamente instalado en el dispositivo móvil de que se trate[101], no sólo tiene la capacidad de acceder a toda la información contenida en el mismo[102], sino, también, **DE EXTRAER DE FORMA REMOTA Y SECRETA DEL DISPOSITIVO MÓVIL ESA INFORMACIÓN Y TRANSMITIRLA PARA SU ANÁLISIS A UN SERVIDOR EN EL QUE AQUÉLLA ES ALOJADA PARA SER REPRODUCIDA EN CUANTO SEA NECESARIO**, podemos concluir que, en el caso que nos ocupa -encontrándose debidamente acreditadas dichas circunstancias-, mi defendido ha sido víctima de una aprehensión virtual mediante la cual fue desposeído de información

[101] *Software malicioso de inteligencia cibernética que, de acuerdo a la evidencia forense aportada al presente escrito, no cabe duda que así ha sido en el caso del dispositivo de mi defendido. Véase, informe "Catalan Gate".*

[102] *En este tramo de la conducta delictiva, vinculada exclusivamente con el apoderamiento de secretos documentales, cabe hacer referencia a que "Pegasus" tiene la capacidad de acceder al listado de contactos del dispositivo, así como también a los archivos, las imágenes, los videos, los correos electrónicos, el historial de navegación web, las contraseñas de acceso, la información bancaria, etc.*

íntima, personal y profesional que desde ya no consentía dar a conocer a los sujetos activos, vulnerándose de esta forma gravemente su intimidad, el secreto de sus comunicaciones y su secreto profesional.

A su vez, y en cuanto a la interceptación de sus telecomunicaciones y la utilización de artificios técnicos de grabación del sonido o captación de la imagen, no cabe duda en este punto que la infección del dispositivo móvil de mi defendido mediante el software de inteligencia cibernética "Pegasus", **también implicó, de acuerdo a la potencialidad del mismo, la interceptación de las llamadas entrantes y salientes, de los mensajes de texto (SMS), de la mensajería instantánea, de aplicaciones como Skype, Whatsapp, Viber, Facebook, etc., así como también la probable grabación de escuchas telefónicas ambientales y la captura de imágenes desde la cámara del dispositivo**, todo lo cual constituye también una grave vulneración a la intimidad de mi representado, que corresponde sea objeto de investigación en la instrucción del sumario que se propicia por esta representación.

Incluso más, se pudo acceder a documentos confidenciales -se trata de un abogado en ejercicio- que, como se dijo, afectan al derecho de defensa de muchas personas, entre ellos varios de los también espiados y, como si eso no fuese

bastante, se pudo introducir en su dispositivo móvil documentos que le perjudiquen a él, a sus defendidos o a terceros sin que lo sepa ni haya participado en la elaboración de los mismos; no se puede hacer una abstracción de un hecho innegable: se ha tratado del espionaje al teléfono móvil de un abogado en ejercicio.

Tampoco puede caber duda, en esta línea argumental que hoy en día, con el avance que ha tenido la tecnología, el acceso y la aprehensión de toda la información que contiene un dispositivo móvil de una persona, desde ya implica una gravísima vulneración a la intimidad, en su máxima expresión, pues el desapoderamiento de aquélla -dada la inmensa cantidad de datos personales y extremadamente sensibles que recopila, procesa y almacena un teléfono móvil inteligente- supone, prácticamente, una privación absoluta de la intimidad.

Además de lo expresado hasta aquí, corresponde ahora pasar a referirnos al delito previsto y penado por el art. 197 bis.1 del Código Penal, toda vez que, como se adelantó en el párrafo inicial de este apartado y como se desarrollará en los siguientes, la significación jurídica de los hechos denunciados no se agota en el delito de descubrimiento de secretos analizado precedentemente.

Esto es así, pues, si se repara en el hecho relativo a que los querellados y/o quienes más eventualmente resulten responsables por aquellos hechos debieron vulnerar las barreras de seguridad establecidas en el dispositivo móvil en cuestión, entendemos que, como medio necesario para cometer el delito aludido, en el caso que nos ocupa, también se ha cometido el delito de acceso ilegal a sistemas de información o de "*intrusismo informático*", en los términos del art. 197 bis.1 del Código Penal. Este tipo penal prevé:

> *"El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años"*.

Este tipo penal, que fue incorporado por primera vez a nuestra legislación por la LO 5/2010 como art. 197.3 del Código Penal, y modificado y reubicado por la LO 1/2015 como art. 197 bis, sanciona el acceso ilegal a sistemas de información.

De acuerdo a lo que establece la Directiva 2013/40/UE[103], normativa que estableció los parámetros en los que se basó la redacción del tipo penal de que se trata, se define a los sistemas de información como:

> "*...todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, protección y mantenimiento...*"[104].

Si bien tradicionalmente se atribuye el concepto de sistema de información a un ordenador, con el avance de la tecnología, en esta definición cabe también incluir a los teléfonos móviles inteligentes, como es el caso que nos ocupa, ya que estos dispositivos, además de tener la capacidad de realizar y recibir llamadas, también son capaces de almacenar, procesar y recuperar enormes cantidades de información de forma automatizada, al igual que los ordenadores tradicionales.

En cuanto se relaciona con los presupuestos que deben ser tenidos en cuenta para tener por configurado el tipo penal de que se

---

[103] Que sustituyó la Decisión marco 2005/222/JAI del Consejo Europeo.
[104] *Véase art. 2.a de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de fecha 12 de agosto de 2013.*

trata, por aquél se requiere un acceso a un sistema de información sin autorización del titular, o la facilitación a otro de ese acceso o mantenimiento en aquél, mediante un quebrantamiento de las medidas de seguridad establecidas para impedirlo, resultando atípicas las conductas de acceso no autorizado a sistemas de información sin protección, o de accesos autorizados por el titular del sistema[105].

En este sentido, por la jurisprudencia se ha establecido que:

> "*...El delito de acceso informático ilícito sanciona el acceso o el facilitar a otro el acceso, sin autorización al conjunto, en nuestro caso, a una parte de un sistema informático y también el mantenimiento dentro del mismo en contra de la voluntad de quien tenga el derecho legítimo a excluirlo.* ***Siendo suficiente para colmar las exigencias del tipo el mero acceso al sistema informático que puede ser directo o remoto pero debe haberse realizado vulnerando las medidas de seguridad establecidas para impedirlo...***"[106].

En función de lo expresado hasta aquí, cabe indicar que, en el caso que nos ocupa, dado que se encontraría acreditada la instalación y la utilización de "Pegasus" en el dispositivo móvil de mi defendido, software malicioso de

---

[105] *ALMENAR PINEDA, F., Delito de hacking. Editorial Aranzadi. 2018.*
[106] *SAP de Madrid Nº 895/17, de fecha 27 de noviembre de 2017.*

inteligencia cibernética que, como se desarrolló por el punto VI.II.A de esta querella, tiene la capacidad de penetrar los dispositivos basados en Android, BlackBerry, iOS y Symbian, así como también los dispositivos protegidos con contraseña o cualquier otra medida de seguridad[107], y además, ello tuvo lugar sin autorización de mi defendido, esta parte entiende que concurren los presupuestos necesarios para concluir que D. Gonzalo Boye fue víctima del delito de acceso ilegal a sistemas informáticos en los términos del art. 197 bis.1 del Código Penal.

Finalmente, el art. 197 quater del Código Penal prevé que:

> *"...Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado..."*.

Los tipos penales de organización o grupo criminal se clasifican dentro de los delitos contra el orden público y, de acuerdo a lo establecido por la LO 5/2010, dicho concepto abarca la seguridad jurídica, la vigencia efectiva del principio de legalidad, los derechos y las libertades de los ciudadanos, todo lo cual,

[107] *Brochure "Pegasus", pág. 3.*

al fin y al cabo, se resume en la calidad de la democracia.

En el caso que nos ocupa, si bien los ataques informáticos instrumentados mediante el software espía "Pegasus" que son el objeto de esta querella se vinculan con aquéllos en los que, exclusivamente, fue víctima mi representado, de todos modos, esto no significa desatender el hecho de que, durante el lapso que tuvieron lugar esos sucesos y de acuerdo a lo revelado al respecto por el reciente informe emitido por The Citizen Lab[108], concurrieron una multiplicidad de ataques informáticos en los que se utilizó este software espía contra los dispositivos móviles de al menos sesenta (65) personas en España -entre las que se encontraba mi representado, abogado en ejercicio y defensor de muchos de los afectados por este espionaje masivo-, con el denominador común que la gran mayoría de ellas se encontraban vinculadas políticamente y/o por el sector de la sociedad que representaban o pertenecían -en este caso, la minoría nacional catalana-, todo lo cual permite presumir, fundadamente, que aquellos ataques habrían sido dirigidos de manera organizada y concertada.

Tal es el caso, sólo por mencionar algunos a título de ejemplo y como ya se ha hecho *ut supra*, de los diputados catalanes del

[108] *Véase, informe completo y gráfico "Catalan Gate".*

Parlamento Europeo que apoyaban la independencia (MEP), Antoni COMIN, Diana RIBA, Jordi SOLÉ, Clara PONSATÍ y Carles PUIGDEMONT[109], así como también de los miembros de la Asamblea Nacional Catalana Jordi SÁNCHEZ, Elisenda PALUZIE y Sònia URPÍ GARCÍA, Meritxell BONET[110], Marcel MAURI[111], políticos catalanes que apoyaban la independencia como el M.H.P. Pere ARAGONÉS y los expresidentes de la Generalitat de Catalunya, por el orden en que fueron depuestos Artur Mas, Carles PUIGDEMONT y Joaquim TORRA, el expresidente del Parlamento de Catalunya Roger TORRENT y la actual presidente de esa cámara Laura BORRÁS, y miembros de los partidos políticos catalanes JUNTS PER CATALUNYA, ESQUERRA REPUBLICANA DE CATALUNYA, CANDIDATURA D'UNITAT POPULAR, PARTIT DEMÒCRATA EUROPEU CATALÀ y PARTIT NACIONALISTA CATALÀ, entre muchos otros.

Bajo estas circunstancias, estimamos que estas amplias, complejas y extendidas en el tiempo operaciones de espionaje informático instrumentadas a los fines de supervisar ilegalmente los procesos políticos catalanes, conductas que, de acuerdo a los argumentos

---

[109] *Las últimas dos personas mencionadas, no fueron afectadas directamente, sino que se infectaron los dispositivos móviles de familiares y/o colaboradores cercanos, práctica de piratería bastante común, que le permite al atacante obtener datos del objetivo principal sin necesidad de acceder al dispositivo de esa persona.*

[110] *Periodista y cónyuge del expresidente de OMNIUM CULTURAL, Jordi CUIXART, fue atacada cuando CUIXART se enfrentaba a cargos por su participación en el referéndum por la independencia de Catalunya de 2017.*

[111] Periodista e historiador y vicepresidente de OMNIUM CULTURAL -luego de que CUIXART fuera condenado el 14 de octubre de 2019 por los hechos relacionados con el referéndum de 2017.

desarrollados *ut supra*, encuentran significación jurídica en el tipo penal previsto y penado en el art. 197.1 del Código Penal y en el art. 197 bis.1 del mismo cuerpo legal, no pudieron haberse llevado adelante sin la existencia de una agrupación estructurada de personas que de manera organizada y concertada, y con carácter estable en el tiempo y una distribución de roles jerárquicos al efecto, lograron ese cometido.

Es por ello que, al menos indiciariamente, entendemos que en el caso que nos ocupa concurren los presupuestos necesarios para concluir que se verifica, además, la circunstancia agravante prevista por el art. 197 quater del Código Penal, toda vez que los hechos delictivos por los cuales fue víctima mi representado habrían sido cometidos en el seno de una organización o de un grupo criminal, según el caso, conformada o conformado, en principio y sin perjuicio del análisis que deberá efectuarse a lo largo de la instrucción a los fines de determinar la adscripción y los roles de aquélla o aquél, por "Q CYBER TECHNOLOGIES L.T.D.", y sus subsidiarias "N.S.O. GROUP TECHNOLOGIES L.T.D." en Israel y "OSY TECHNOLOGIES S.à.r.l." en Luxemburgo, así como también de Niv KARMI, de Shalev HULIO y Omri LAVIE, entre muchos otros que deberán ser individualizados a lo largo de esta investigación.

VIII – DILIGENCIAS QUE SE INTERESAN

1. Se tome declaración al querellante,

2. Se tome declaración, en calidad de peritos, a los expertos de Citizen Lab, John SCOTT-RAILTON, Bill MARCZAK, Bahr Abdul RAZZAK, Siena ANSTIS, Gözde Böcü, Salvatore SOLIMANO y Rono DEIBERT, autores del informe pericial que se adjunta a la presente querella,

3. Se remita atento oficio al Parlamento Europeo para que aporte y se incorporen al presente procedimiento los vídeos del evento organizado por el Partido Popular Europeo en dicha institución el pasado 10/02/2022[112].

4. Que se citen a declarar en calidad de testigos a Laurent RICHARD, Sandrine RIGAUD, Roman Jacek GIERTYCH, Máté SZABÓ, Bill MARCZAK y Krzysztof BREJZA, que han participado en el evento organizado por

[112] *Véase, a estos efectos, el vídeo del evento:LIVE: Pegasus spyware scandal and its impact on democracy in the EU*

el Partido Popular Europeo en el Parlamento Europeo el pasado 10/02/2022.

5. Que a través del punto neutro judicial se recaben todos los datos económicos y bancarios que existan en España respecto a los querellados D. Niv KARMI, D. Shalev HULIO y D. Omri LAVIE así como de las mercantiles igualmente querelladas "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D.", y "OSY TECHNOLOGIES S.à.r.l."

6. Que se solicite al Banco de España para que informe de cualquier transferencia de dinero que se haya realizado desde el sistema bancario español y a favor de D. Niv KARMI, D. Shalev HULIO y D. Omri LAVIE así como de las mercantiles igualmente querelladas "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D."

7. Se interesa que, a través de la oportuna comisión rogatoria internacional o, preferentemente, con desplazamiento de una comisión judicial a Israel y en

virtud de lo establecido en los arts. 3 y 4 del Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959, y del art. 2 del Segundo Protocolo Adicional a dicho convenio, hecho en la ciudad mencionada el 8 de noviembre de 2001[113] para que:

> A.- Se notifique la presente querella y se tome declaración en calidad de investigados a D. Niv KARMI, D. Shalev HULIO, D. Omri LAVIE y a quienes ostenten la representación legal de "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D.", todos estos últimos también en calidad de investigados,
>
> B.- Se requiera a la representación legal de las empresas "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D." para que aporten la documentación acreditativa de todos los contratos, convenios o cualquier clase de acuerdo que se haya

[113] *Ambos convenios fueron suscriptos por el estado de Israel.*

suscripto con el gobierno de España, el Centro Nacional de Inteligencia o cualquier organismo/empresa público español o empresa privada española o que trabaje con entidades españolas, para el uso del software malicioso de inteligencia cibernética "Pegasus" en el territorio español,

C.- Se solicite de las autoridades israelíes acceso a toda la información bancaria referida a las empresas israelíes "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D." a fin de determinar **pagos y dineros relacionados, exclusivamente, con empresas, personas o entidades públicas españolas o con aquellas que hayan tenido como origen inicial España o servicios prestados hacia España,**

D.- Se solicite de las autoridades israelíes toda la información de la que dispongan de viajes a España de los

querellados D. Niv KARMI, D. Shalev HULIO y D. Omri LAVIE así de cualesquiera otros empleados o trabajadores de las empresas querelladas "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D." con expresa indicación de las fechas en que se produjeron los mismos,

E.- Se requiera igualmente de las autoridades israelíes cualquier otro dato de movimientos migratorios hacia Israel por parte de ciudadanos españoles que hayan mantenido relaciones comerciales o de cualquier otro tipo con las empresas querelladas "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" y TECHNOLOGIES L.T.D." y/o con los querellados D. Niv KARMI, D. Shalev HULIO y D. Omri LAVIE,

F.- Se requiera igualmente de las autoridades israelíes para que informe de cuáles autorizaciones de prestación de servicios y/o venta de material

informático y/o aplicaciones informáticas se han concedido a las mercantiles "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" en relación con empresas, agencias estatales y/o personas de nacionalidad española o que fuesen a prestar dichos servicios o vender ese material informático y/o aplicaciones informáticas para su uso en España o desde o hacia España,

8. Que al amparo de lo previsto en la DIRECTIVA 2014/41/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 3 de abril de 2014 relativa a la orden europea de investigación en materia penal se solicite a las autoridades judiciales de Luxemburgo para que:
    A. Se notifique y tome declaración en calidad de investigados a quienes ostenten la representación legal de "OSY TECHNOLOGIES S.à.r.l.", en calidad de investigados,
    B. Se requiera a la representación legal de las

empresas “OSY TECHNOLOGIES S.à.r.l.” para que aporten la documentación acreditativa de los contratos, convenios o cualquier clase de acuerdo que se haya suscripto con el gobierno de España, el Centro Nacional de Inteligencia o cualquier organismo/empresa público español o empresa privada española o que trabaje con entidades españolas, para el uso del software malicioso de inteligencia cibernética “Pegasus” en el territorio español.

C. Se requiera al conjunto de entidades bancarias que operan en Luxemburgo o a la autoridad supervisora bancaria belga para que informen sobre la existencia de cualesquiera cuentas bancarias, depósitos, cajas de seguridad o cualquier otro tipo de activos financieros que aparezcan

bajo titularidad de "OSY TECHNOLOGIES S.à.r.l.", "Q CYBER TECHNOLOGIES L.T.D.", "N.S.O. GROUP" o TECHNOLOGIES L.T.D.", y según el caso, que aporten los resúmenes de cuenta correspondientes, desde el año 2014 al 2021, ambos inclusive.

D. Se requiera al conjunto de entidades bancarias que operan en Luxemburgo para que informen sobre la existencia de cualesquiera cuentas bancarias, depósitos, cajas de seguridad o cualquier otro tipo de activos financieros que aparezcan bajo titularidad de D. Niv KARMI, D. Shalev HULIO, D. Omri LAVIE, y según el caso, que aporten los resúmenes de cuenta correspondientes, desde el año 2014 al 2021, ambos inclusive.

E. Se requiera a las autoridades de Luxemburgo

para que investiguen cualquier transferencia que, procedente de España, se haya realizado a las cuentas bancarias de las empresas antes mencionadas,

9. Se aporte la hoja histórica penal de los querellados.

Y todas aquellas otras diligencias que se desprendan de las anteriores.

Por todo lo anterior,

SOLICITO AL JUZGADO: Que teniendo por presentado este escrito de querella, junto con las copias y los documentos que se acompañan, se sirva **admitirla a trámite y acuerde practicar las diligencias solicitadas en el cuerpo de este escrito**.

Es Justicia que pido en Madrid, a 3.05.2022

PRIMER OTROSÍ DIGO: Que si, a pesar de venir firmada la presente querella por parte, también, del propio querellante, se considera necesario se le requiera a través de esta representación para que la ratifique apud acta o aporte poder especial para querella.

SEGUNDO OTROSÍ DIGO: Se agrega a la presente querella, en relación con los documentos a los cuales se hizo referencia a lo largo de esta presentación, el siguiente índice:

INDICE DOCUMENTAL:

Número de anexo	**Descripción**	**Número de páginas**
Doc. 1	Brochure de "Pegasus", elaborado por NSO.	4
Doc. 2	Artículo periodístico: *Qué es "Pegasus": así funciona el software de espía israelí que hackea a medio mundo*	13
Doc. 3	Complaint NSO.pdf	111
Doc. 4	Artículo periodístico: *El escándalo del programa Pegasus desata la sospecha de un estado policial en Israel*	14
Doc. 5	Artículo periodístico: *Israeli spyware company accused of hacking activists hires lobby firm*.	12

Doc. 6	Artículo periodístico: *El millonario israelí que vende software espía a medio mundo para colarse en tu móvil - El Confidencial*	20
Doc. 7	Artículo periodístico: *The battle of the most powerful cyberweapon*	20
Doc. 8	Reporte de NSO GROUP	32
Doc. 9	Extracto del Registro de Comercio de Luxemburgo con relación a "OSY TECHNOLOGIES"	4
Doc. 10	Artículo periodístico: *¿Qué es el Pegasus Project?*	24
Doc. 11	Anexos Técnicos del contrato de adquisición de "Pegasus" por parte de la Procuraduría General de la República de México (2 documentos).	46 y 51, respectivamente.
Doc. 12	Artículo periodístico: .*Pegasus Project: la red de empresas que vendió "Pegasus" al gobierno de Peña Nieto*.	31
Doc. 13	Artículo periodístico: *Quién es quién de las víctimas de los teléfonos infectados por Pegasus*	6
Doc. 14	Artículo periodístico: *Pegasus project: el espionaje de los regímenes autoritarios al desnudo.*	15
Doc. 15	Informe de The Citizen Lab: Project Torogoz, acerca del espionaje masivo de Pegasus en El Salvador.	24
Doc. 16	Artículo periodístico: .*Bukele pactó con la pandilla M-13 en El Salvador*	12
Doc. 17	Artículo periodístico: Rajoy pide un "candidato limpio" para la generalitat. ABC.	4

Doc. 18	Informe completo de The Citizen Lab: *"Catalan Gate"*	49
Doc. 19	Informe gráfico de The Citizen Lab acerca del "Catalan Gate": ¿Harías clic?	33
Doc. 20	Artículo de wikipedia acerca de la *Operación Vóljov*	6
Doc. 21	*The Supervisor*, recorte de la página web del Supervisor Europeo de Protección de Datos.	2
Doc. 22	Informe del Supervisor Europeo de Protección de Datos "*EDPS Preliminary Remarks on Modern Spyware | European Data Protection Supervisor*".	12
Doc. 23	Video de la audiencia pública organizada por el Partido Popular en el Parlamento Europeo el 10/02/2022: *LIVE: Pegasus spyware scandal and its impact on democracy in the EU*	
Doc. 24	Artículo periodístico: *How Democracies Spy on their Citizens*	26

Por ser Justicia que pido en lugar y fecha *ut supra*.