DG 49561/25

Escrito de interposición de querella.

AL JUZGADO DE INSTRUCCIÓN DE BARCELONA

QUE POR TURNO DE REPARTO CORRRESPONDA

[redacted], Procuradora de los Tribunales y de **D. JOAN ARÚS SAN SEGUNDO, D. JORDI BAYLINA MELE, D. PAU ESCRICH GARCIA, D. JOAN MATAMALA I ALZINA y D. XAVIER VIVES RIBA,** actuando todos ellos bajo la defensa letrada de los letrados del ICAB Xavier Muñoz Soriano y Alejandro Gámez Selma, Cdos. [redacted] y [redacted], respectivamente, según acreditamos con los apoderamientos notariales y apud acta digitales específicos para interponer querella adjuntos como **Doc. 1.1 a 1.6**, ante este Juzgado comparezco y, como mejor proceda en derecho, digo

Que, por medio del presente escrito y en representación de los antedichos vengo a interponer **QUERELLA** por la presunta comisión de los delitos de **Descubrimiento y revelación de secretos informáticos del 197.2 CP, de acceso ilegal a sistemas informáticos del 197BIS CP**, con las agravantes de haber sido realizados por autoridades y funcionarios públicos y por grupo criminal, así como cualquier otro delito que pueda deducirse durante la investigación de los presentes hechos contra **D. Felix Vicente Azón Vilas** y **Dña. María Gámez Gámez**, ambos exDirectores Generales de la Guardia Civil, **Dña. Paz Esteban López**, ExSecretaria de Estado Directora del Centro Nacional de Inteligencia, **SAITO TECH, LTD** (Antes denominada Candiru LTD, con sede en Israel), **NSO GROUP TECHNOLOGIES LTD** (Sede en Israel), **OSY Technologies Sarl** (Sede en Luxemburgo), **Q Cyber Technologies Sarl** (Sede en Luxemburgo) y sus representantes legales y directivos **D. Shalev Hulio, D. Yuval Somekh, D. Eran Shorer, D. Ya'akov Weizman, D. Eitan Achlow,**

PRIMERO – JUZGADO ANTE EL QUE SE PRESENTA

Esta querella se presenta ante los Juzgados de Instrucción de Barcelona por ser competentes de conformidad con los artículos 14.2, 17.2, 18.1 LECrim y 84 y 88.1.a) LOPJ.

En efecto, nos encontramos ante **delitos conexos en virtud del art 17.2.a) y b) LECrim**: "*2. A los efectos de la atribución de jurisdicción y de la distribución de la competencia se consideran delitos conexos:*

1.º Los cometidos por dos o más personas reunidas.

2.º Los cometidos por dos o más personas en distintos lugares o tiempos si hubiera precedido concierto para ello."

Y el posterior art. 17.2, segundo párrafo, nos señala que *"los delitos conexos serán investigados y enjuiciados en la misma causa cuando la investigación y la prueba en conjunto de los hechos resulten convenientes para su esclarecimiento y para la determinación de las responsabilidades procedentes salvo que suponga excesiva complejidad o dilación para el proceso."*

Y es que los delitos aquí reseñados han sido cometidos de concierto por un grupo organizado de personas dentro de la Administración española con el soporte tecnológico imprescindible de empresas extranjeras, quienes consideraron en su momento que los querellados, todos ellos informáticos y programadores, tomaron parte en el desarrollo y programación de las herramientas informáticas que promovieron la difusión de la plataforma "Tsunami Democràtic".

Los lazos comunes entre las víctimas y los delitos aquí señalados aconsejan, tanto por tiempo como por recursos económicos, una investigación conjunta:

A) Todos los ofendidos pertenecen al colectivo de empresarios de la tecnología y fueron espiados ilegalmente por las mismas razones;

B) Todos fueron objeto de investigación judicial conjunta en la misma causa

judicial en la Audiencia Nacional;

C) La querella se dirige contra los mismos querellados y por los mismos delitos.

Una vez acreditada la naturaleza conexa de los delitos por los que nos querellamos y la eficiencia que supone agruparlas en una sola causa, queda resolver el Juzgado competente para ello.

Señala el art. 18 LECrim que es competente para conocer de los delitos conexos con preferencia aquel del territorio en que se haya cometido el delito con mayor pena o, subsidiariamente, el que primero comenzare a conocer de la causa.

El Acuerdo del Pleno no Jurisdiccional de la Sala Segunda del Tribunal Supremo, en reunión de fecha 3 de febrero de 2005, estableció que: "*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa*". Cabe añadir que el TS viene considerando que el delito informático, que normalmente se comete desde un ignorado lugar y produce sus efectos en diversas ubicaciones geográficas, es perseguible en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado.

En el presente caso, dos de los cinco querellantes tienen domicilio en la ciudad de Barcelona (D. Joan Arus San Segundo y D. Pau Escrich García), mientras que D. Xavier Vives está domiciliado en Igualada, en la misma provincia. El Sr. Jordi Baylina directamente no tiene domicilio en España.

A mayor abundamiento, de las investigaciones hechas por la Guardia Civil a las que hacemos mención en el cuerpo de esta querella, se desprende que la parte mayoritaria de estos espionajes tuvieron lugar cuando los querellantes se encontraban físicamente en Barcelona.

Finalmente, los delitos aquí expuestos no están siendo objeto de investigación en ningún otro foro judicial.

SEGUNDO.- NOMBRE Y DOMICILIO DE LOS QUERELLANTES.

Los querellantes son:

- **JORDI BAYLINA MELE**, mayor de edad, con DNI [redacted]
- **JOAN ARÚS SAN SEGUNDO**, mayor de edad, con DNI [redacted]
- **PAU ESCRICH GARCIA**, mayor de edad, con DNI [redacted]
- **JOAN MATAMALA I ALZINA**, mayor de edad, con DNI [redacted]
- **XAVIER VIVES RIBA**, mayor de edad, con DNI [redacted]

TERCERO.- NOMBRE Y DOMICILIO DE LOS QUERELLADOS.

Los querellados son:

- **Félix Vicente Azón Vilas**, ExDirector General de la Guardia Civil entre el 29/06/2018 y el 18/01/2020, con domicilio a estos efectos en la sede social de ésta, sita en [redacted] Madrid

- **María Gámez Gámez**, ExDirectora General de la Guardia Civil entre el

18/01/2020 y el 28/03/2023, con domicilio a estos efectos en la sede social de ésta, sita en [redacted] Madrid

- **Paz Esteban López,** ExSecretaria de Estado - Directora del Centro Nacional de Inteligencia, entre el 06/07/2019 y el 11/05/2022, con domicilio a efectos de notificaciones en la sede social de éste, sito en la [redacted]

- **NSO GROUP TECHNOLOGIES Ltd**, con domicilio declarado en Galgalei Haplada, 22, Herzliya, 4672222, Israel.

- **Q CYBER TECHNOLOGIES Ltd;** con domicilio en Galgalei Haplada, 22, Herzliya, 4672222, Israel.

- **OSY TECHNOLOGIES Sarl**, filial de la primera, con domicilio en Rue Edward Steichen, 2, Luxemburgo, código postal 2540.

- **Q CYBER TECHNOLOGIES Sarl**, filial de la primera, con domicilio en Rue Edward Steichen, 2, Luxemburgo, código postal 2540.

- **SAITO TECH Ltd**, anteriormente conocida como Candiru Ltd, con sede en Israel pero domicilio desconocido.

- **Shalev Hulio**, fundador de la empresa matriz NSO Group Technologies Ltd y actual consejero delegado y directivo de las dos filiales luxemburguesas, con domicilio a efectos de notificaciones en [redacted].

- **Yuval Somekh**, directivo de ambas filiales luxemburguesas entre 2016 y 2020, con domicilio a efectos de notificaciones en [redacted]

- **Eran Shorer**, fundador y directivo de Saito Tech Ltd, con domicilio

desconocido en Israel.

- **Ya'akov Weizman**, fundador y directivo de Saito Tech Ltd, con domicilio desconocido en Israel.
- **Eitan Achlow,** actual CEO de Saito Tech, Ltd, con domicilio desconocido en Israel.

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

CUARTO.- RELACIÓN CIRCUNSTANCIADA DE LOS HECHOS.

Primero.- Del uso global de este spyware y su utilización en España.

En Julio de 2.021 fue publicado por el Grupo Universitario The Citizen Lab, basado en la Universidad de Toronto, Canada, el informe "*Hooking Candiru*", hecho en colaboración con Microsoft Threat Intelligence Center. Este informe no sólo acreditaba que en España se había utilizado este Spyware sino que recoge la localización, detección y examen del primer caso de infección "*en vivo*" de *Candiru* del mundo, infección hecha sobre nuestro representado D. Joan Matamala. Gracias a esta detección precoz y en directo, la propia Microsoft pudo desarrollar el software necesario para cerrar -por un tiempo- la brecha de seguridad en su sistema operativo que había permitido la infección de más de 100 terminales de víctimas en varios países del mundo. Este informe es el **Doc. 2**.

Al año siguiente, 2022, fue publicado por el mismo Grupo Universitario el informe "*CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*", **que acreditaba indubitadamente que, como mínimo, 65 personas en España habían sido infectadas o sufrido intentos de infección en sus**

teléfonos móviles y portátiles desde el año 2015 hasta el año 2021[1] por dos programas de spyware denominados *Pegasus* y *Candiru*. Este informe es el **Doc. 3**.

En concreto, al menos 63 de esas personas fueron atacadas y/o infectadas con Pegasus, 4 con Candiru y 2 con ambos programas de spyware -Justo los actuales querellantes-.

Entre las personas infectadas y no participantes en esta querella se encuentran Carles Puigdemont, Quim Torra y Pere Aragones, ex-Presidents de la Generalitat de Catalunya; los exDiputados del Parlamento Europeo Antoni Comin y Clara Ponsatí; los senadores y diputados del Congreso Miriam Nogueras, Teresa Rivero, Assumpció Castellvi; los ExPresidents del Parlament de Catalunya Roger Torrent y Laura Borràs, los letrados de varios de los anteriores Gonzalo Boye, Andreu Van der Eynde o Jaume Alonso-Cuevillas, o miembros de la sociedad civil en Catañunya como Maritxell Bonet, Marcel Mauri o Elena Jiménez.

Amnistía Internacional ha corroborado y confirmado a través de un informe forensic posterior (**Doc. 4**) la realidad de las infecciones detectadas por The Citizen Lab, pues entre los terminales reexaminados por el Departamento Forense de esta organización se encuentran cuatro terminales ya analizados por The Citizen Lab cuyos resultados concuerdan con los resultados obtenidos por éste.

Y es que este informe tan preciso de *The Citizen Lab* se sumaba a las ya numerosas denuncias públicas por utilización ilegal de estos programas por todo el mundo, desde que en julio de 2021 Amnistía Internacional y el consorcio de periodistas *Forbidden Stories* sacaran a la luz que al menos 50.000 teléfonos habían sido infectados por todo el orbe con este spyware, en uno de los ataques más masivos e intensos a la privacidad que se conocen.[2]

---

1 Se detectó también un intento de infección por Pegasus ya en el año 2015. La útima infección detectada ha sido a Joan Matamala en el año 2.021.

2 a) https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/pegasus-espionaje-masivo/
b)https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/proyecto-pegasus-una-filtracion-de-datos-masiva-revela-que-el-software-espia-de-la-empresa-israeli-nso-group-se-utiliza-para-atacar-a-activistas-periodistas-y-figuras-politicas-en-todo-el-mundo/

Así, se han reportado casos de infección a ciudadanos de Azerbaiyán, India, Hungría, Marruecos, Turquía, Méjico, El Salvador, Francia, Sáhara Occidental, Bahrein, Palestina, Israel, Iran, Líbano, Yémen, Reino Unido, Turquía, Armenia o Singapur.

En España, además de las 67 personas identificadas fehacientemente por The Citizen Lab, se han descubierto con posterioridad también infecciones con Pegasus al Presidente del Gobierno de España, Pedro Sánchez, a los ministros de Interior o Defensa o al periodista especializado en Magreb y Mashrech, Ignacio Cembrero.

También han confirmado el informe de The Citizen Lab, es decir, la realidad de las infecciones, **varios informes del cuerpo de Mossos d'Esquadra** en dos procedimientos judiciales diferentes. En el iniciado por D. Jordi Sánchez, Dña. Elizenda Paluzie y Dña. Sònia Urpí el informe policial señala que las infecciones empezaron ya en 2.015[3], y en el iniciado por D. Pere Aragonès, los agentes han corroborado que su móvil sufrió ataques del spyware Pegasus entre 2018 y 2020[4] . Fuera, por tanto, de las fechas reconocidas por el CNI de haber empleado Pegasus con autorización judicial.

Este espionaje a unos niveles nunca vistos, tanto en la intensidad de la intimidad despojada como en el nº de víctimas y alcance internacional, provocó la creación de una Comisión de Investigación en el Parlamento Europeo, la Comisión Pega, cuyo informe final de 15/06/2023 adjuntamos como **Doc. 5** y cuyas conclusiones específicamente dirigidas a España (Punto 22 del Informe) son relevantes para este Tribunal puesto que señalan que:

> - El Gobierno español debe llevar a cabo una investigación completa, justa y eficaz, en la que se proporcione total claridad sobre todos los presuntos casos de uso de software espía, incluidos los 47 casos en los que aún no está determinado si fueron o no objetivo del CNI con autorización judicial o si lo fueron de otra autoridad española con o sin autorización judicial.

3 https://www.abc.es/espana/cataluna/pegasus-mossos-certifican-espionaje-exlider-junts-jordi-20241127142033-nt.html?ref=https%3A%2F%2Fwww.google.com%2F

4 https://elpais.com/espana/catalunya/2024-12-19/los-mossos-certifican-que-el-movil-de-aragones-fue-espiado-con-pegasus-sin-aval-judicial.html

- El Gobierno español debe facilitar un acceso adecuado a las 18 personas investigadas reconocidas por el CNI a las autorizaciones judiciales que habilitaban dichas intromisiones.

- El Gobierno español debe colaborar con la Administración de Justicia española para garantizar que las personas atacadas con software espía tengan acceso a recursos legales reales y significativos, y para que las investigaciones judiciales puedan concluir sin demora de forma imparcial y exhaustiva, para lo cual deben asignarse recursos suficientes.

- El Gobierno español debería invitar a Europol a colaborar en estas investigaciones aportando su conocimiento técnico.

El 2 de febrero de 2023 los Relatores Especiales de la ONU sobre el derecho de reunión y de asociación (Sr. Fernando de Varennes) y sobre el derecho de opinión y expresión (Sra. Irene Khan) emitieron un comunicado conjunto en el que solicitaban a las autoridades españolas que llevaran a cabo "*una investigación completa, justa y efectiva sobre estas acusaciones, publicar las conclusiones y detener cualquier interferencia ilegal en los derechos fundamentales de los activistas de la minoría catalana en España.*"[5]

El 15/03/2024 compareció en el Parlament de Catalunya D. Donncha Ó Cearbhaill, Director del Laboratorio Forensic de Amnistía Internacional que había confeccionado el Informe ya aportado como **Doc. 6.** Este experto en seguridad digital aseguró que este software es tan invasivo que no es compatible con ningún estándar actual de protección del derecho fundamental a la intimidad y a la privacidad. Reflexión que este mismo Tribunal debe en parte compartir toda vez que el debate sobre el lugar procesal en el que ha de regularse la autorización para la instalación de este software, si análogo a la intervención telefónico o comparable por su intromisión a la entrada y registro de vivienda, está de plena actualidad en el derecho procesal español actual.

A la misma conclusión llega el Supervisor Europeo de Protección de Datos (EPDS) cuando afirma en su informe de 11/04/2017 "Manual para la evaluación de la

5 https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting

necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal" (**Doc. 7**) que:

> *"El Tribunal de Justicia afirma que «... si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha».*
>
> *También afirma que solo la lucha contra la delincuencia grave podría justificar la conservación selectiva y el acceso a los datos de las comunicaciones electrónicas. « Habida cuenta de la gravedad de la injerencia en los derechos fundamentales afectados que supone una normativa nacional que prevé, a efectos de la lucha contra la delincuencia, la conservación de datos de tráfico y de localización, sólo la lucha contra la delincuentica grave puede justificar una medida de este tipo». «Además, dado que el objetivo perseguido por dicha normativa debe guardar una relación con la gravedad de la injerencia en los derechos fundamentales que supone este acceso, de ello se deriva que, en materia de prevención, investigación, descubrimiento y persecución dr delitos, sólo la lucha contra la delincuencia grave puede justificar dicho acceso a los datos conservados»"*

Segundo.- Del contexto en el que se producen estos espionajes a los querellantes.

Apartado Primero.- De la participación del CNI.

Aunque en la fecha de publicación del segundo informe de *The Citizen Lab* (Julio 2022) no podía afirmarse con rotundidad que el Gobierno Español era el cliente

responsable de este espionaje -pese a las evidentes circunstancias que lo sugerían-, a día de hoy estamos en condiciones de afirmar rotundamente que sí lo es en tanto en cuanto el propio Centro Nacional de Inteligencia ha confirmado su contratación y utilización en la comparecencia de su entonces Directora, Dña. Paz Esteban López, ante la Comisión de Secretos Oficiales del Congreso de los Diputados de 05/05/2022.

No obstante, este reconocimiento es parcial y limitado por cuanto la compareciente sólo reconoció esta intromisión total en la intimidad de 18 de las 63 personas confirmadas por The Citizen Lab de haber sido infectadas por el spyware Pegasus y además por unos plazos de tiempo inferiores a los que The Citizen Lab ha acreditado, según conocemos por las revelaciones hechas por el diario "La Vanguardia". El CNI, además, reconoció haber utilizado el spyware Pegasus contra otras 7 u 8 personas no citadas en el Informe de The Citizen Lab, pero tachó sus nombres.[6]

Dña. Paz Esteban ya se encuentra investigada en tres procedimientos abiertos por el uso de Pegasus sin autorización judicial[7], en uno de lso cuales recientemente los Mossos d'Esquadra han aportado una prueba pericial que confirmaría las infecciones del querellante desde julio de 2018, cuando Paz Esteban era Secretaria General del Centro, que entonces dirigia D. Félix Sanz Roldán.

De la utilización del spyware Candiru, sin embargo, el CNI ha guardado estricto silencio, sin reconocerlo ni negarlo. Tampoco ninguna otra autoridad española ha reconocido su utilización hasta la fecha, pese a estar acreditado su uso contra cuatro de los querellantes.

Según señalaba La Vanguardia en la noticia mencionada, cuatro de los 7 u 8 nombres tachados por el CNI durante la comparecencia de Dña. Paz Esteban en la Comisión de Secretos Oficiales corresponden con los creadores del protocolo de voto digital Vocdoni. Extremo corroborado por otra noticia de El Confidencial[8]: "*El Centro*

6 https://www.lavanguardia.com/politica/20220514/8266136/18-espiados-cni-pegasus.amp.html

7 https://efe.com/cataluna/2025-02-14/la-exdirectora-del-cni-paz-esteban-investigada-en-una-tercera-causa-por-espionaje-a-erc-con-pegasus/

8 https://www.elconfidencial.com/espana/2022-04-29/pegasus-espionaje-cni-tsunami-democratic-vocdoni-referendum_3416269/

Nacional de Inteligencia (CNI) investigó por orden del Gobierno al autor del informe de Citizen Lab sobre Pegasus y a otros tres ingenieros por su papel en las protestas contra la sentencia del 1-O. " y "*Al menos cuatro de los individuos que aparecen en el informe de Citizen Lab hecho público la semana pasada, incluido su autor, Elies Campo, participaron en la creación de un protocolo de voto digital de alta seguridad para ser utilizado en un nuevo referéndum secesionista.*". Y "*Miquel, Baylina, Escrich y el propio Campo aparecen en la lista de Citizen Lab. Como reveló El Confidencial, forman parte de los 18 individuos implicados en Tsunami Democràtic y los contactos internacionales con el Kremlin*[9] *que fueron investigados por el Centro Nacional de Inteligencia (CNI) con supervisión judicial y con la autorización del Gobierno.*" Dado que cuatro de los querellantes sí aparecen en el Informe de The Citizen Lab y en la lista del CNI (Jordi Baylina, Joan Matamala, Pau Escrich y Xavier Vives), resulta fácilmente factible que entre los cuatro nombres no revelados del grupo de "*los creadores del programa Vocdoni*" se encuentre el otro querellado (Joan Arús), pues formó parte de este reducidísimo grupo de desarrolladores de software y fue también objeto de investigación judicial en la Audiencia Nacional. Lamentablemente, el Sr. Arus perdió el móvil antes de poder ser examinado por The Citizen Lab.

Siendo pública e indiscutida la mayor de las cuestiones (Que el Centro Nacional de Inteligencia sí utilizó spyware Pegasus contra un colectivo de personas relacionados con el proceso de independencia de Catalunya, y en concreto contra 25 personas entre los cuales se encuentran los actuales querellantes Baylina, Matamala, Escrich y Vives), y aunque no podemos realizar ninguna afirmación categórica ulterior por hallarnos sepultados bajo el denso manto de la Ley de Secretos Oficiales, esto ya es indicio suficiente para iniciar las presentes pesquisas y averiguar qué autoridad realizó las instalaciones del spyware antes y después de los plazos admitidos por el CNI y contra personas no admitidas por el CNI. De ahí que corresponda a este Juzgado el realizar las solicitudes pertinentes de desclasificación de secretos a fin de conocer la identidad y extensión de la intromisión en la intimidad de los querellantes por parte de las autoridades españolas así como el correspondiente juicio de legalidad sobre la

9 Aunque de la participación del Kremlin el artículo no dice nada, sólo lo deja intencionadamente caer.

motivación aducida para ello, en caso de existir.

Durante la visita de los integrantes de la Comisión Pega del Parlamento Europeo a España, resulta relevante la entrevista oficial realizada a D. Miguel González, uno de los periodistas que más ha informado sobre el uso de este spyware en España, quien señala que:

> *El Sr. González hizo hincapié además en que sigue sin poder explicarse la diferencia entre dieciocho y sesenta y cinco casos pero que, si la directora del CNI admitió dieciocho, también podría haber admitido sesenta y cinco. Añadió que las escuchas se descubrieron gracias a Citizen Lab y, al haberse confirmado dieciocho casos detectados por Citizen Lab, ya no tiene sentido seguir cuestionando la responsabilidad de su análisis. Mencionó que una forma de explicar la divergencia de cifras podría ser también que Pegasus fuera utilizado por más de una agencia y que los casos restantes no fueran responsabilidad del CNI.*

Es el **Doc. 8.**

Apartado Segundo.- De la participación de la Guardia Civil.

Todos los querellantes fueron objeto de seguimientos e investigación a lo largo de varios años desde el 2019 bajo las DDPP 99/2018 del Juzgado Central de Instrucción nº 6 (Caso "Tsunami Democratic") e igualmente objeto de investigación en las DDPP 85/2019 del mismo Juzgado (*Caso Judas*; donde Vocdoni -plataforma de voto digital creada por varios de los querellantes- aparece como investigada a lo largo de 92 folios). No obstante, tras las investigaciones a ninguno le fue imputado delito alguno ni les fue comunicada su condición de investigados ya que tras conocer que estaban siendo espiados, solicitaron personarse en dichas diligencias en varias ocasiones, siéndoles denegado el derecho a defenderse.

En el marco de las DDPP 85/2019 mencionadas fue incoada la Pieza Separada 1,

secreta, donde fueron autorizadas por el Juzgado Central 6 diversas medidas de intervención de las comunicaciones sobre los querellantes. Estas intervenciones fueron asignadas para su realización y verificación a la Unidad Central Especial 3 de la de la Jefatura de Información de la Dirección General de la Guardia Civil, cuyo mando ostentaron durante los años 2019 y 2020 el Sr. Félix Vicente Azón Vilas primero (Hasta el 18/01/2020) y la Sra. María Gámez Gámez (A partir del 19/01/2020), de forma que los delitos por los que nos querellamos se produjeron con su consentimiento y/o tolerancia, pues resulta impensable que estas medidas tan invasivas y sin autorización judicial se realizaran sin su conocimiento ni aprobación previa.

Las medidas de investigación autorizadas por este Juzgado Central sobre los querellantes, prorrogadas mensual o bimensualmente y ejecutadas por la Unidad Central Especial 3, fueron las siguientes, de menor a mayor intrusión en su intimidad:

A) Intervenciones telefónicas, que incluían también el envío y recepción de los datos GPRS, IMTS, "*debiendo servir la información en doble canal (estereo), verificándose la grabación y conservación de las conversaciones por el sistema SITEL",* todo ello durante los los siguientes plazos:

- Jordi Baylina Mele y Joan Matamala i Alzina, del 16 de diciembre de 2019 al 16 de julio de 2020.

- Elíes Campo Cid, del 16 de enero de 2020 al 16 de julio de 2020.

- Pau Escrich García y Joan Arus San Segundo, del 16 de marzo de 2020 al 16 de julio de 2020.

B) Intervención de los IMEI de las líneas telefónicas de los querellantes, durante los siguientes plazos:

- Jordi Baylina Mele y Joan Matamala i Alzina, del 16 de enero de 2020 al 16 de julio de 2020.

- Pau Escrich García y Joan Arus San Segundo, del 16 de mayo de 2020 al

16 de julio de 2020.

C) Autorización para *"la instalación de un software que permita, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de los terminales de los investigados."* **Esto es, Pegasus y/o Candiru y/o otro spyware de similares características.**

Según los autos judiciales "*Este software, tras su instalación en los diferentes dispositivos informáticos/telefónicos, procederá a enviar mediante tecnología de conmutación de paquetes de datos encriptados,para garantizar la confidencialidad, al Sistema de Interceptación de Telecomunicaciones de la Guardia Civil la información necesaria para la investigación.*

Dicho software, permitirá acceder a la siguiente información:

- *Acceso a la agenda de contactos.*

- *Acceso al registro de video-llamadas o llamadas IP.*

- *Cuenta de correo asociada al terminal.*

- *Acceso a las comunicaciones a través de las citadas cuentas.*

- *Historial de navegación web.*

- *Comunicaciones en redes sociales, aplicaciones de mensajería y chats, así como el histórico de las mismas.*

- *Árbol de archivos.*

- *Ficheros almacenados en el sistema de archivos del terminal en cualquier formato que se presenten.*

Respecto de la posibilidad de activación del micrófono instalado en el

dispositivo, con la finalidad de captar y grabar las comunicaciones orales, deberá presentarse la expresa solicitud conforme al artículo 588 quater a. (Que no nos consta, de momento, que se haya producido)

Ello durante los siguientes plazos:

- Jordi Baylina Mele y Joan Matamala i Alzina, del 16 de enero de 2020 al 17 de julio de 2020.

Además de las anteriores, la Unidad Central Especial 3 de la Guardia Civil realizó una exhaustiva investigación de los querellantes mediante medidas no necesitadas de autorización judicial previa, como seguimientos fotográficos, vigilancias, consultas de vuelos tomados por los querellantes o sus familiares, consultas en registros públicos, etc como admiten directa e indirectamente en los sucesivos Oficios 14668 del 2019 y 340, 351, 1.292, 3.027, 3.078, 3.090, 4.584, 4.617 y 4.618 del 2020.

Así, aunque la Guardia Civil ha asegurado no utilizar el spyware Pegasus por boca del Ministro del Interior, existen indicios suficientes para afirmar que ha utilizado tanto *Pegasus* como *Candiru*:

A) La gran mayoría de las infecciones y/o intentos de infección sufridos por los querellantes, aunque comienzan todas antes de las autorizaciones judiciales ya señaladas, sí se detienen precisamente en julio de 2017, al mismo tiempo que deja de prorrogarse la autorización judicial para el uso de un software "q*ue permita, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de los terminales de los investigados"* en las DDPP 85/2019 (Caso Tsunami Democratic), autorización cuya realización ya hemso visto que encomendó el Juzgado a la UCE3 de la Guardia Civil.

B) El 10 de enero de 2020 se producen dos intentos de infección con spyware *Candiru* a los querellantes Xavier Vives y Pau Escrich. Justo ese día se reunieron los querellantes Pau Escrich y Joan Arus con otra víctima de este espionaje (el Sr. Elíes Campo), en el domicilio del Sr. Arus; una reunión que el Oficio 3078/2020,

de 12 de marzo, de la UCE3 recoge como particularmente "sospechosa" pues hizo seguimiento fotográfico de la misma y la cita en diversas ocasiones en el Informe. Los querellantes habían hablado días antes por canales de mensajería y teléfono de organizar esta reunión, por lo que hay una conexión directa entre la celebración de esta reunión tan importante para la Guardia Civil y los intentos de infección para conocer su contenido.

C) El ya mencionado Elíes Campo, que ya hemso señalado que también fue objeto de intento d einfección según recoge el informe de The Citizen Lab, fue fotografiado por la Guardia Civil llegando al Aeropuerto de Barcelona desde Estados Unidos el 18/12/202019 (Oficio 340/2020, de 10/01, de la pieza Separada Secreta 1 d las DDPP 85/19). El Sr. Campo había sufrido un intento de infección con *Candiru* el 05/12/2019 pero ninguno por *Pegasus* puesto que su terminal y nº de teléfono es estadounidense, país en el que NSO Group tiene vetado en principio utilizar spyware. Pero justo el mismo día de su llegada, vigilada por la Benemérita, es infectado por Pegasus su padre, D. Elias Campo Guerra. Su madre María Cinta lo fue el día anterior, pero también el 19, el 23, el 28, el 30 de diciembre de 2019 y varias veces más en Enero de 2020. El CNI ha negado haber intervenido los teléfonos de estas tres personas, aunque en cambio Elíes Campo era objetivo prioritario de investigación de la Guardia Civil, como los sucesivos oficios policiales dejan meridianamente claro.

Por tanto, respecto de la Guardia Civil sólo consta un periodo en que tenían autorización judicial para emplear este spyware y sólo respecto de Jordi Baylina y Joan Matamala. **El periodo anterior y posterior, así como la extensión a otros querellantes no tiene habilitación judicial en las DDPP 85/19**. Ello sin perjuicio que ninguna orden judicial hubiera autorizado espiar a los familiares del Sr. Elíes Campo, puesto que nada tenían que ver con los hechos ni existía justificación para tan gravosa vulneración de su intimidad.

QUINTO.- De la naturaleza y alcance de la intromisión del spyware Pegasus y Candiru

A) PEGASUS.

El programa espía **Pegasus** es un software de inteligencia diseñado para infiltrarse de manera remota y discreta en dispositivos móviles, permitiendo la extracción ilimitada de información. Este sistema recopila, organiza y transmite los datos obtenidos para su análisis, funcionando como una herramienta integral de vigilancia. Desde 2012, Israel lo ha clasificado como un arma de inteligencia cibernética. Aunque se permite su comercialización, esta está restringida a entidades públicas o agencias estatales previamente autorizadas por el Ministerio de Defensa israelí. Entre los países que han adquirido Pegasus se encuentran España, Suiza, Grecia, Hungría, Polonia o Chipre, pero no Estados Unidos.

Adjuntamos la descripción del producto hecha por la propia NSO Technologies, la desarrolladora, como **Doc. 9**.

Pegasus es capaz de infectar dispositivos con sistemas operativos como Android, BlackBerry, iOS, Symbian y Windows, incluso si estos cuentan con contraseñas de protección. Su instalación se lleva a cabo de forma remota mediante tecnología "over-the-air" sin necesidad de interacción del usuario ("Zero click"), lo que deja mínimas huellas en el dispositivo afectado. En los casos en que no pueda ejecutarse remotamente, el software también puede instalarse a través de un enlace malicioso enviado por mensaje de texto (SMS), emails o mensajes de canales de mensajería (Whatsapp, Telegram, Signal, etc). Si la víctima accede al enlace, el software intenta desplegarse localizando alguna vulnerabilidad en el software del terminal. Si lo localiza, descarga el paquete informático y toma el control del dispositivo.

Una vez instalado, Pegasus obtiene acceso completo al dispositivo, replicando sus funcionalidades. Sus capacidades incluyen:

- Interceptar llamadas de voz y VoIP en tiempo real.

- Extraer información como contactos, archivos, imágenes, videos, contraseñas, mensajes (SMS y mensajería instantánea), correos electrónicos, registros de calendario, y el historial de navegación web.
- Capturar imágenes y videos desde la cámara, y grabar audio mediante el micrófono del dispositivo.
- Monitorear aplicaciones como Skype, WhatsApp, Viber, Facebook y BlackBerry Messenger (BBM).
- Localizar al usuario mediante GPS para rastrear su ubicación exacta.
- Operar independientemente del proveedor de servicios móviles, sin requerir cooperación de los operadores de red.
- Continuar vigilando el dispositivo incluso si se cambian identidades virtuales o tarjetas SIM.

La recopilación de datos que realiza Pegasus es casi ilimitada, estructurada en tres niveles según NSO Group:

1. **Extracción inicial**: Una vez instalado, el software transmite el historial de mensajes, contactos, llamadas, registros de calendario, correos electrónicos, historial de navegación web y otros datos del dispositivo.
2. **Monitoreo pasivo**: Tras la extracción inicial, Pegasus sigue recopilando nueva información en tiempo real, como mensajes, llamadas y actividades del dispositivo, utilizando tecnologías como "Cell-ID".
3. **Recopilación activa**: A solicitud, el sistema puede ejecutar tareas específicas en tiempo real, como rastrear la ubicación del objetivo mediante GPS, interceptar llamadas, recuperar archivos, realizar grabaciones de sonido ambiental, capturar imágenes o tomar capturas de pantalla.

   Además de esta asombrosa y terrible capacidad para extraer de forma remota y

secreta la información del dispositivo móvil y transmitir esa información para su análisis, Pegasus puede analizar los datos recogidos y así enviar alertas a a los operadores del spyware tras la llegada de datos importantes para marcar eventos importantes, **así como para alterar, introducir y extraer documentos del dispositivo atacado**.

Respecto de la información obtenida, esta es almacenada **en los propios servidores de NSO Group y desde ahí son renviados a sus clientes**. No obstante, ignoramos en qué servidores concretos son alojados, las medidas de seguridad de éstos, las condiciones de alojamiento ni el responsable de su custodia, ni si los mismos son utilizados, onerosa o gratuitamente, por la propia NSO una vez es facilitada al cliente (por ejemplo, podría revender datos desagregados a terceros o utilizarlos internamente con fines estadísticos y de desarrollo y mejora del propio spyware).

En una resolución histórica, de 20/12/2024, NSO Group ha sido condenada en Estados Unidos por acceder ilegalmente a la plataforma de mesnjería Whattsapp, tras la correspondiente demanda presentada por esta plataforma en defensa de sus usuarios espíados. Una vez reconocido en sentencia que el acceso era ilegal, sólo queda por determinar la extensión de lso daños y perjuicios.[10]

B) CANDIRU.

En esencia y en lo que es relevante para esta querella, Candiru tiene la misma operabilidad, funcionamiento y fines que Pegasus. Candiru (Identificado en algunos informes como "Sourgum") es un producto desarrollado por la empresa también israelí Saito Tech Ltd, fundada por antiguos accionistas y directivos de NSO Group. Su objetivo principal es, de nuevo, infiltrarse en dispositivos tecnológicos con el fin de monitorizar las comunicaciones del objetivo, extraer datos sensibles y rastrear sus actividades, todo ello sin el conocimiento del afectado.

Recordemos que toda la información recogida en este apartado sobre el modo de

10 https://www.washingtonpost.com/technology/2024/12/20/whatsapp-meta-nso-pegasus-hacking-spyware/

operar y funcionalidades de Candiru la conocemos gracias que The Citizen Lab pudo detectar una infección "en vivo y en directo" en el ordenador del queerellante Joan Matamala y estudiarla sin que los operadores del spyware fueran alertados. Gracias a esta detección precoz, The Citizen Lab alertó a Microsoft y ésta pudo cerrar la brecha de seguridad que había explotado Candiiru para infectar más de 100 terminales de víctimas en varios países del mundo, garantizando asá la seguridad -durante un tiempo- de cientos de millones de usuarios en todo el mundo.

Comercialmente Candiru es la marca patentada por su empresa desarrolladora, Saito Tech Ltd, siendo Devil's Tongue el nombre expecífico del programa.

A diferencia de Pegasus, Candiru SÍ puede infectar otras plataformas, no sólo móviles, sino también tablets, portátiles, PCs, etc.

Entre sus funciones principales cabe señalar:

- **Recolección de información personal y sensible:** Candiru puede obtener contraseñas, credenciales de acceso, historiales de navegación, mensajes de texto, correos electrónicos y listas de contactos.

- **Monitorización de comunicaciones en tiempo real:** Facilita la interceptación de llamadas de voz, videollamadas y mensajes encriptados enviados mediante aplicaciones seguras, incluyendo Whatsapp, Telegram y Signal.

- **Acceso al micrófono y cámara del dispositivo:** El software es capaz de activar, sin la detección del usuario, el micrófono o la cámara para grabar conversaciones, videos o tomar fotografías del entorno.

- **Rastreo de ubicación y actividad:** El spyware puede obtener datos GPS, registrar las posiciones del dispositivo a lo largo del tiempo y generar un mapa detallado de los desplazamientos del objetivo.

- **Persistencia y escalamiento de privilegios:** Una vez instalado, Candiru puede

operar de manera encubierta y lograr persistir en el dispositivo, evitando la detección o eliminación; además, puede aprovechar vulnerabilidades del sistema operativo para elevar sus privilegios.

Técnicamente, su modo de operar es diferente al de Pegasus. Candiru suele utilizar "exploits" para fallos desconocidos en navegadores (como Chrome o Safari), así como en sistemas operativos (Windows, macOS, iOS, Android), con el fin de infectar el dispositivo sin requerir interacción significativa del usuario (Zero-click). Para ello se vale de la distribución de enlaces trampa o archivos adjuntos infectados que, al ser simplemente abiertos, inician silenciosamente la instalación del spyware.

Dado que Candiru utiliza una red muy vasta de servidores, dominios y direcciones IP para disfrazar las comunicaciones entre dispositivo infectado y atacante, el rastreo de este spyware es particularmente complicado.

Candiru es un spyware altamente sofisticado y flexible, diseñado para permitir un acceso extenso y en la práctica ilimitado al terminal de la víctima. Permite extraer contenidos del mismo, buscar en sus navegadores historial y accesos pasados y hasta robar mensajes encriptados en otras herramientas informáticas. Al igual que Pegasus, Candiru es capaz de utilizar remotamente los programas en la nube asociados al terminal y de enviar o colgar mensajes y posts en las redes sociales y apps vinculadas, haciendo pasar al operador del spyware como el usuario del dispositivo, **lo que le convierte además en un vector muy peligroso para introducir pruebas falsas en contra de la víctima.** [11]

Según el precio ofrecido por la propia empresa en una oferta comercial que se filtró públicamente (**Doc. 10**), el **precio inicial de Candiru es de 16 millones de euros**. Por este precio se permiten un número ilimitado de infecciones pero el control y

11 "Microsoft's analysis also established that the spyware could send messages from logged-in email and social media accounts directly on the victim's computer. This could allow malicious links or other messages to be sent directly from a compromised user's computer. Proving that the compromised user did not send the message could be quite challenging." https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/
"DevilsTongue can also send messages as the victim on some of these websites, appearing to any recipient that the victim had sent these messages. The capability to send messages could be weaponized to send malicious links to more victims." https://www.microsoft.com/en-us/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

monitorización de sólo 10 terminales infectados al mismo tiempo. Por 1,5 millones adicionales Saito Tech permite monitorizar otros 15 terminales a la vez y por 5,5 millones se aumenta a 25 terminales adicionales y se extiende a 5 países.

Por 1,5 millones adicionales, los clientes pueden adquirir la posibilidad de activar cualquier comando o función en el terminal infectado, una función particularmente peligrosa pues podría sevir para introducir pruebas falsas en el terminal (Como descargar archivos o enviar mensajes por cualquier aplicación todo ello sin conocimiento del usuario)

La información pública sobre el domicilio social exacto de Candiru, conocida actualmente como Saito Tech Ltd., es extremadamente limitada. Candiru es una empresa israelí dedicada al desarrollo y venta de herramientas de ciberespionaje y, a diferencia de compañías con mayor exposición, como NSO Groop, mantiene una política de privacidad absoluta: No tiene web, no figura en registros ni listados web, no emite comunicados de prensa, no se anuncia públicamente y sus 120 empleados tienen prohibido revelar en redes sociales que trabajan para ésta, además de firmar extensos acuerdos de confidencialidad.[12]

Pese a que varias investigaciones independientes (como la realizada por Citizen Lab) y numerosos reportajes periodísticos en medios internacionales lo han intentado, resulta muy complejo hallar la sede social exacta de Saito Tech Ltd, más allá de saber que está radicada en Tel Aviv, Israel. Ello porque en Israel el acceso a ciertos datos de su Registro Mercantil (Registrar of Companies) es restringido.

12 https://www.haaretz.com/middle-east-news/2019-01-04/ty-article/.premium/top-secret-israeli-cyberattack-firm-revealed/0000017f-e36d-d38f-a57f-e77ff84b0000

SEXTO.- De la acreditación indubitada del espionaje sufrido por los querellantes usando los anteriores dos spywares.

Los aquí querellantes forman parte todos de la comunidad internacional de desarrollo de software para la democratización de las sociedades, tanto a nivel práctico como académico. Esta comunidad realiza investigaciones y estudios, así como desarrolla programas de software, que permite aprovechar las potencialidades del internet, la tecnología y el software libre para promover una mejor democracia a través de una mayor participación de la ciudadanía en el espacio público y en la toma de decisiones gubernamentales por vías digitales. Entre estas herramientas ha de mencionarse, por ser relevante como justificación del espionaje dada por las autoridades españolas, el programa *Vocdoni,* un programa de voto digital extremadamente seguro desarrollado por algunos de los aquí querellantes.

Analicemos uno por uno a los querellantes y sus diversas infecciones y extracciones sufridas:

1.- JORDI BAYLINA.

Este querellante es desarrollador jefe y cofundador de Polygon, una plataforma diseñada para mejorar la escalabilidad y eficiencia de Ethereum mediante soluciones de Capa 2. Entre sus principales productos se encuentran Polygon PoS y Polygon zkEVM, cada uno con características y casos de uso específico . También es asesor en proyectos relacionados con el voto digital y en proyectos de descentralización y de privacidad.

Baylina fue ampliamente atacado con Pegasus, recibiendo al menos **26 infecciones exitosas**. Al final, se infectó al menos **ocho veces entre el 29 de octubre de 2019 y el 11 de julio de 2020.**

Según la Causa DDPP 85/19 del Juzgado Central 6 de la Audiencia Nacional, la utilización de este spyware contra él fue autorizada entre el 16/01/2020 y el 17/07/2020. Por tanto, las infecciones de spyware acreditadas por Baylina a través del

informe de The Citizen Lab finalizan al mismo tiempo que finalizan las autorizaciones judiciales concedidas a la UCE3, -pese a que comenzaron mucho antes-.

Baylina fue también objeto de vigilancia física desde, al menos, el 18/12/2019 por la UCE3 de la Guardia Civil y sometido a intervención telefónica y del IMEI del 16 de diciembre de 2019 al 17 de julio de 2020.

El CNI ha reconocido haber usado el spyware Pegasus contra él, pero ignoramos tanto la motivación como las fechas, así como la existencia, motivación y proporcionalidad de la correspondiente autorización judicial conforme al art. 12 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Entre otras formas de ser infectado, Baylina recibió un SMS falso que fingía ser el enlace a una tarjeta de embarque de un vuelo internacional de las aerolíneas suizas (Swissair) que había comprado previamente. Esto indica que el propio spyware podría haber tenido acceso ante al Registro de nombres de pasajeros (PNR) de Swissair u otra información similar del transportista.

Otra forma utilizada por Pegasus fue fingir SMS de la Hacienda y Seguridad Social españolas, bajo los títulos de AEAT y Segsocial, los cuales hasta recogían parcialmente el DNI del Sr. Baylina para ofrecer más veracidad al engaño.

Igualmente recibió varios SMS fingiendo ser invitaciones al Mobile World Congress.

2.- JOAN MATAMALA I ALZINA.

Este querellante resulta relevante, pues es el denominado "paciente cero" de las infecciones con *Candiru*, **el primero al que se le pudo detectar una infección en vivo de este Spyware, en julio de 2021**. No obstante, además de *Candiru* Matamala fue objeto de ataques informáticos exitosos con Pegasus en, al menos, 16 ocasiones entre el 07 de agosto de 2019 y el 13 de julio de 2020.

Según la Causa DDPP 85/19 del Juzgado Central 6 de la Audiencia Nacional, la utilización de este spyware contra él fue autorizada entre el 16 de enero de 2020 y el 17 de julio de 2020. No obstante, la propia Guardia Civil señala en la causa que en todo este periodo **no logró tener éxito en la instalación de este spyware en su terminal.**

Joan Matamala fue también objeto de vigilancia física desde el 18/12/2019 por la UCE3 de la Guardia civil y sometido a intervención telefónica y del IMEI del 16e diciembre de 2019 al 17 de julio de 2020.

El CNI ha reconocido haber usado el spyware Pegasus contra él, pero ignoramos tanto la motivación como las fechas, así como la existencia, motivación y proporcionalidad de la correspondiente autorización judicial conforme al art. 12 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

3. XAVIER VIVES.

Vives es cofundador de *Vocdoni*. Vives fue atacado por *Candiru* a través del envío de mails y de SMS que simulaban ser avisos del Gobierno de España relacionados con novedades y recomendaciones sobre la pandemia de Covid 19.

Así, fue atacado hasta cinco veces entre el 10/01/2020 y el 17/02/2020, y una más esporádica en octubre de 2020.

Sobre Vives no nos consta ninguna autorización judicial para la utilización de este software de espionaje, pero sí fue objeto de profuso seguimiento e investigación durante las DDPP 85/2019 por agentes de la UCE3 de la Guardia Civil, como reflejan varios de los oficios policiales allí presentados.

El CNI ha reconocido haber usado el spyware Pegasus contra él, pero ignoramos tanto la motivación como las fechas, así como la existencia, motivación y proporcionalidad de la correspondiente autorización judicial conforme al art. 12 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

4. PAU ESCRICH.

Escrich es también cofundador de *Vocdoni* y experto en desarrollo de código abierto.

Escrich fue atacado por *Candiru* hasta en 5 ocasiones entre el 10/12/2019 y el 04/02/2020, mediante mails falsos que simulaban ser entradas para el *Mobile World Congress,* al que nuestro representado acude cada año. El hecho de que tanto Escrich como Baylina sufrieran un ataque tan similar sugiere que los autores criminales son los mismos.

Igualmente consta que Escrich sufrió un intento de infección por *Pegasus*, sin éxito, el 02/06/2020.

Sobre Escrich no nos consta ninguna autorización judicial para la utilización de software espía pero sí fue objeto de profuso seguimiento durante las DDPP 85/2019, tanto físicamente por agentes de la UCE3 de la Guardia Civil como mediante intervenciones telefónicas y del IMEI que se prolongaron del 16 de marzo al 16 de julio de 2020.

El CNI ha reconocido haber usado el spyware Pegasus contra él, pero ignoramos tanto la motivación como las fechas, así como la existencia, motivación y proporcionalidad de la correspondiente autorización judicial conforme al art. 12 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

5.- JOAN ARÚS SAN SEGUNDO.

El Sr. Arús es empresario tecnológico y co-fundador del proyecto Vocdoni junto con Xavier Vives y Pau Escrich, así como impulsor y desarrollador de software de gobernanza digital y participación política.

Aunque no constan su nombre en el Informe de *The Citizen Lab* ni poseemos evidencias forenses de la infección de su terminal, ya que le sustrajeron el terminal poco antes de que *The Citizen Lab* comenzara a examinar los terminales de las víctimas, existen indicios que apuntan a que sí lo fue.

Por un lado, el Sr. Arús comparte la misma posición de investigado que el Sr. Escrich en las DDPP 85/2019, Pieza Separada 1. Esto es, fue sujeto a un dispositivo de vigilancia personal y a investigación en fuentes abiertas por la Benemérita y a intervenciones telefónicas y del IMEI autorizadas judicialmente del 16 de marzo al 16 de julio de 2020.

Por otro lado, en la comparecencia del 05/05/2022 en la Comisión de Secretos Oficiales del Congreso de los Diputados, la exDirectora del CNI, Dña. Paz Esteban, señaló que el CNI había utilizado el software Pegasus para investigar a 25 personas, de las cuales sólo identificó a 18 con nombres y apellidos.

Pero entre los no identificados el periódico La Vanguardia cita que "*en los documentos aportados aparecían siete u ocho nombres tachados, correspondientes a otras tantas personas sobre las que el espionaje fue autorizado y que escaparon al análisis de Citizen Lab* [...] *Cuatro o cinco de los nombres eliminados forman parte del entorno tecnológico que el CNI vincula a Tsunami Democratic* [...]"[13] Y dado que el resto de personas principales "*del entorno tecnológico*" son precisamente el resto de querellados cuyo espionaje sí ha sido reconocido por el CNI, es lógico suponer que Joan Arús, persona también principal en la creación de *Vocdoni*, sea uno de esos 4 o 5 nombres adicionales tachados.

6. Otras utilizaciones de spyware relevantes para esta causa.

Pese a no ser qurellante, resulta importante señalar la situación de D. Elíes Campo Cid y su familia, pues permite vislumbrar la gravedad de la ilegalidad en la

13 https://www.lavanguardia.com/politica/20220514/8266136/18-espiados-cni-pegasus.html

utilización de estos programas de spyware.

El Sr. Elies Campo, conocido y colaborador en proyectos tecnológicos con los querellantes, también fue objeto de un intento de infección por *Candiru* mediante mail el 05 de diciembre de 2019 cuando estaba físicamente en EE.UU, donde vivía y aún vive. No pudo ser infectado por *Pegasus* puesto que, entendemos, por política comercial NSO Group tiene prohibido infectar dispositivos estadounidenses. El mail trampa simulaba ser un envío informativo del Registro Mercantil de Barcelona.

Dado que el intento de infección no fue exitoso, **los querellados cambiaron de estrategia y procedieron a infectar los móviles de sus familiares directos que sí residían en España, nada más aterrizar éste en España** De ese modo, entre el 16/12/2020 y el 15/01/2020, los padres del Sr. Campo, los Sres [redacted] y [redacted], así como su hermana, sufrieron 13 intentos de infección, la mayoría exitosos. Todo ello consta acreditado en el informe de The Citizen Lab.

Sobre el Sr. Campos no nos consta ninguna autorización judicial para el uso de spyware contra él, pero al igual que los anteriores, fue objeto de profusa investigación personal, seguimientos e intervención telefónica del 16 de enero al 16 de julio de 2020 en el marco de las DDPP 85/2019 del Juzgado Central 6 (*Caso Tsunami Democratic*). Hasta el punto de que en los oficios policiales incluyen una fotografía, tomada por los propios agentes, del Sr. Campo a su llegada al aeropuerto del Prat el 18 de diciembre de 2019.

El CNI ha reconocido expresamente no haberle investigado con spyware en ningún momento.

Por supuesto, sobre ninguno de sus familiares consta solicitud alguna de espionaje, ni del CNI ni de la Guardia Civil, dado que ninguna orden judicial hubiera autorizado espiar a los familiares del "investigado" Elíes Campo, pues nada tenían que ver con los hechos, ni existía justificación para tan gravosa vulneración de su intimidad.

SÉPTIMO.- DELITOS INDICIARIAMENTE COMETIDOS.

Primero.- Delito de descubrimiento y revelación de secretos informáticos. (Art. 197.2 CP)

El art. 197.2 se encuentra ubicado en el capítulo primero "Del descubrimiento y revelación de secretos, del Título X del Libro II del Código Penal que se rotula como "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". Garantizados por el artículo 18.1 CE, estos derechos salvaguardan un espacio de intimidad personal y familiar que debe estar libre de intromisiones, especialmente ante el avance de tecnologías que pueden capturar y difundir información personal.

Por intimidad, por tanto, se pueden entender diversos conceptos que vienen a coincidir en la existencia de una esfera de privacidad que permite a las personas excluir a terceros de su conocimiento. El Código actual ha hecho además especial referencia a la llamada "*libertad informática*", ante la necesidad de conceder a la persona facultades de control sobre sus datos en una sociedad informatizada, siguiendo en su origen las pautas de la ya derogada Ley Orgánica de Regulación del tratamiento Automatizado de Datos personas (LORTAD) 5/92 de 29.10, relacionada con el Convenio del Consejo de Europa de 28/01/81, y la Directiva 95/46 del Parlamento de la Unión Europea relativos a la protección de tales datos y a su libre circulación.

Esta segunda dimensión de la intimidad conocida como **libertad informática o habeas data**, encuentra su apoyo en el **art. 18.4 CE**, en donde taxativamente se dispone que "*la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". Esto implica un derecho a la autodeterminación informativa, permitiendo a las personas decidir qué datos pueden ser recopilados y tratados informáticamente (habeas data), así como oponerse a su uso para fines no autorizados distintos de aquél legítimo que justificó su obtención (SSTC. 11/98 de 13.1 o 45/99 de 22.3).

En este sentido, la STS 358/2007 de 30 de abril destacó al analizar el art. 197.1 CP que dicho precepto contiene varias conductas en su compleja redacción y sanciona

expresamente a quien interceptare las comunicaciones de otro y al que utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen o de cualquier otra señal de comunicación, en todos los casos sin consentimiento de la víctima y con la finalidad de descubrir sus secretos o vulnerar su intimidad. Estas conductas no precisan que el autor llegue a alcanzar la finalidad perseguida. Pero mientras en la primera conducta se requiere un acto de apoderamiento o de interceptación efectivos, en el supuesto de utilización de artificios basta con la creación del peligro que supone su empleo con las finalidades expresadas para la consumación de la infracción penal. **De ahí que en el presente caso hayan de sancionarse tanto las infecciones exitosas como las infructuosas.**

También sanciona el art. 197.2 CP a quien, sin estar autorizado, se apodere, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Así como a quien simplemente acceda a ellos por cualquier medio sin estar autorizado y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

El **bien jurídico protegido es la intimidad individual**. Aunque la idea de secreto **puede ser más amplia**, como conocimiento solo al alcance de unos pocos, en realidad éstos deben estar vinculados precisamente a la intimidad pues esa es la finalidad protectora del tipo. En este sentido, la STS nº 666/2006, de 19 de junio, en la que se dice que "*la idea de secreto en el art. 197, 1º CP resulta conceptualmente indisociable de la de intimidad: ese "ámbito propio y reservado frente a la acción y el conocimiento de los demás" (SSTC 73/1982 y 57/1994 entre muchas)*".

En relación a la **conducta** enjuiciada, interesa resaltar que el tipo objetivo requiere solamente el mero acceso de los datos protegidos en el segundo. El **tipo subjetivo** exige, naturalmente, el dolo en el acto de apoderamiento o de acceso.

Centrándonos en el análisis de los delitos recogidos en el art. 197.2, éstos tienen un sentido claramente distinto a los recogidos en primer punto, ya que las conductas

afectan a datos que no están en la esfera de custodia del titular, sino en bancos de datos y que por tanto pueden causar perjuicios a terceros distintos del propio sujeto al que se refiere la información concernida.

Un sector doctrinal considera que **en el art. 197.2 se protegen, en realidad, dos bienes jurídicos**. Por una parte, la **intimidad del sujeto pasivo**, en relación con las conductas de apoderarse, acceder y utilizar los datos. Por otra parte, la **integridad de los datos**, en relación con los comportamientos de modificar o alterar. Distinción, no obstante, relativa por el hecho de quien pretende modificar o alterar, primero debe acceder, con lo que se habría lesionado también la intimidad en estas modalidades de conducta.

Consecuentemente, como ya hemos indicado, lo que se protege en este apartado segundo es la **libertad informática** entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, lo que constituye una dimensión positiva de la intimidad que constituye el bien jurídico protegido.

Advierte la doctrina que **el calificativo de reservado carece en absoluto de sentido**, debiendo descartarse -como después se analizará más extensamente- la tesis de que la protección penal haya de limitarse a solo cierto tipo de datos personales de mayor relevancia, con exclusión de otros, cuya protección quedaría reservada al ámbito administrativo. Prueba de que ello no es así lo proporciona el apartado 5° que agrava la pena que corresponde a las conductas realizadas sobre esos datos de especial relieve, lo que evidencia que los demás están incluidos dentro del apartado 2. Por ello en el sentido del tipo el entendimiento más adecuado del carácter reservado de los datos es considerar que son tales los que no son susceptibles de ser conocidos por cualquiera. El precepto insiste en ello al aclarar por partida doble que el delito lo comete el que accede a los datos o los utiliza "sin estar autorizado", evidencia de que no son datos al alcance de cualquiera.

Los datos, además, han de estar "*recogidos (registrados) en ficheros o soportes*

informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado". Fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (art. 3 b. LPDP) y conforme al art. 4.6 del Reglamento (UE/2016/679 del Parlamento Europeo y del Consejo de 27-4-2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE) , fichero es "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o repartido de forma funcional o geográfica".

En el sentido del art. 197.2 CP debe exigirse que se trate de un conjunto organizado de información relativa a una generalidad de personas. Dado el carácter reservado de los datos, los ficheros o registros han de ser de acceso y utilización limitada a personas concretas y con finalidades específicas, siendo indiferente, su naturaleza: personal, académica o laboral, medica, económica, etc... Se trata, en realidad de informaciones de carácter personal relacionadas más con la privacidad que con la intimidad. No tienen por qué ser informativos, porque se acoge también a cualquier otro tipo de archivo o registro público o privado. Las conductas van dirigidas a datos que se hallen registrados, es decir a bancos de datos preexistentes, entendiéndose por la doctrina que no es típica la creación clandestina de bancos de datos, que queda en el ámbito administrativo sancionador.

Las conductas tienen que producirse sin estar autorizado para acceder, manipular o modificar el banco de datos y realizarse en perjuicio de tercero, tercero que puede ser distinto al titular de los datos produciéndose una triple implicación de sujetos (sujeto activo, titular de los datos y eventual perjudicado) que responde a la idea de que el titular de los datos no puede ser sujeto activo del delito porque él es el sujeto pasivo, dado que lo tutelado es su intimidad, tal como precisa la STS.1461/2001 de 11 de julio.

a) En principio, todos los datos personales automatizados, son "sensibles" porque las diferentes leyes que hemos tenido en este campo (LORTAD, LOPD y actual LOPDGDD) no distinguen a la hora de ofrecerles protección. Cualquer datos, en

principio inocuo al ser informatizado, puede ser objeto de manipulación, permitiendo la obtención de información.

No existen, por consiguiente, datos personales automatizados reservados y no reservados, **por lo que debe interpretarse que todos los datos personales automatizados quedan protegidos por la comunicación punitiva del art. 197.2 CP.**

c) No es posible, a su vez, interpretar que "los datos reservados" son únicamente lo más sensibles, comprendidos en el "núcleo duro de la privacidad", (v.g. ideología, creencias, etc.) para quedar los no reservados en el grupo de los sancionables administrativamente, por cuanto dicho enfoque hermenéutico chocaría con una interpretación sistemática del art. 197 CP, ya que si en él se prevé un tipo agravado para esta clase de datos (numero 5) "a sensu contrario" los datos tutelados en el tipo básico, serían los no especialmente protegidos (o "no reservados") en la terminología de la Ley.

En consecuencia y en línea de principio, no importa la trascendencia e importancia objetiva de los datos personales y familiares. No cabe, pues, diferenciar a efectos de protección entre datos o elementos "objetivamente" relevantes para la intimidad que serían los únicos susceptibles de protección penal y datos "inocuos" cuya escasa significación los situaría directamente fuera de la intimidad penalmente protegida. En esta dirección la STS 725/2004 de 11 de junio nos dice que el art. 197. 2 CP no hace distinciones respecto del objeto de la acción que tengan fundamento en normas no penales y se refiere a "datos reservados de carácter personal o familiar" registrados en soportes informáticos, electrónicos o telemáticos de archivos o registros públicos o privados. Es decir, que el legislador ha querido alcanzar todos los datos de estas características porque, indudablemente, todos son merecedores de protección penal.

Ahora bien, sí debe exigirse que los datos o información pertenezcan al ámbito privado y personal o familiar del sujeto. La STS 358/2007 de 30 de abril, recordó que, aunque en el segundo apartado del art. 197 se refiere a datos reservados de carácter personal o familiar, no siendo preciso que pertenezcan al núcleo duro de la privacidad, pues de ser así se aplicaría la agravación del apartado quinto del artículo 197, sí es

necesario que afecten a la intimidad personal.

Hay que distinguir entre la irrelevancia "objetiva" del contenido e **importancia de la información para que la protección penal opere en el caso de datos de carácter personal o familiar**, a que se refiere el art. 197.2, que, desde el punto de vista sustancial y aisladamente considerados, son generalmente inocuos; y la **necesaria equiparación que debe establecerse entre "secreto" y "reservados" a efectos de la intimidad personal y familiar**. En efecto de una interpretación teleológica y sistemática se debe concluir que el término "reservados" que utiliza el Código hay que entenderlo como "Secretos" o "no públicos", parificándose de este modo el concepto con el art. 197.1 CP. Secreto será lo desconocido u oculto, refiriéndose a todo conocimiento reservado que el sujeto activo no conozca o no esté seguro de conocer y que el sujeto pasivo no desea que se conozca.

Y en cuanto **al "perjuicio de tercero" es el elemento que más problemas ocasiona en relación al tipo que nos ocupa**.

Ante la polémica doctrinal sobre si tal expresión debe considerarse un elemento subjetivo del injusto, o exige efectivamente la producción del resultado, la STS 234/1999 de 18 de febrero mantuvo que el perjuicio producido por la acción tiene que estar naturalmente abarcado por el dolo, pero no tiene que ser el único ni el prioritario móvil de la acción. Llegó a esta conclusión no sólo a partir de la ubicación sistemática del artículo 197.2, sino también de la propia relevancia constitucional del bien jurídico lesionado por el delito, cuya protección penal no puede estar condicionada, so pena de verse convertida prácticamente en ilusoria, por la improbable hipótesis de que se acredite, en quien atente contra él, el deliberado y especial propósito de lesionarlo.

Para la STS 1084/2010 subjetivamente se exige que la conducta se lleve a cabo en perjuicio de tercero, aunque no haya un ánimo especifico de perjudicar. Y basta con que la acción se realice con la finalidad dicha, sin que resulte necesaria para la consumación la producción del resultado lesivo. "**Se trata por tanto de un delito de peligro que no requiere la ulterior producción de un resultado de lesión**". En este caso, además

hemos de entender que el perjuicio existió pues, el acusado con su acción puso al descubierto los datos obrantes en las bases en cuestión, cuyo carácter reservado está fuera de toda duda, y con ello dañó el derecho de sus titulares a mantenerlos secretos u ocultos (en este sentido se pronunció la STS 990/2012, de 18 de octubre)".

Segundo.- Del delito de acceso ilícito a sistemas informáticos (Art. 197bis CP)

Realiza la conducta típica de este delito quien accede a un sistema informático ajeno, sin consentimiento de su titular y vulnerando las medidas de seguridad, aunque sea sin intención alguna de realizar ningún mal posterior. Con respecto al acceso, puede ser tanto a la totalidad o a parte del sistema, y tendrá que haber sido realizado de forma no autorizada y vulnerando las medidas de seguridad establecidas para impedirlo, quedando fuera del tipo tanto los accesos que se efectúen gozando de una autorización legal o judicial a tal efecto (art. 588 septies LECrim), como los que se realicen con el consentimiento de la persona que está legitimada para acceder al sistema.

Una vez que la medida se haya vulnerado y el sujeto haya accedido de forma dolosa al sistema, se habrá completado el injusto típico de este delito, lo que determinará su consumación. El mero intento de vulneración de la medida de seguridad o su elusión no seguida del efectivo acceso al sistema en cuestión solo se podrá sancionar mediante la apreciación de la tentativa de delito, pues nos encontramos ante un delito de resultado.

En lo que respecta a la segunda modalidad comisiva de este artículo ("f*acilite a otro el acceso al conjunto o una parte de un sistema de información*"), se añade para garantizar así que el facilitador sea castigado expresamente como autor y además en su forma consumada, con independencia de si el tercero a quien pretendía ayudar a acceder al sistema ajeno de forma no autorizada consiguiese hacerlo o no.

Respecto al bien jurídico protegido, este delito viene a proteger **el derecho que tiene toda persona a conservar al margen de intromisiones no deseadas determinados espacios digitales en los que almacenan y procesan sus datos**

informáticos. Un derecho que tiene por finalidad garantizar a su titular que podrá tratar en dicho espacio los datos que estime pertinente con la garantía de estar penalmente protegido frente a posibles intromisiones con el fin de garantizarle el seguro ejercicio de su vida privada y la intimidad en determinados espacios, aun cuando no los hubiese empleado aún de forma efectiva para ejercitarlos.

Tercero.- Tipo agravado para autoridades y funcionarios públicos (Art. 198 CP) o, alternativamente, delito de interceptación ilegal de las telecomunicaciones (Art. 536 CP).

En virtud del art. 198 CP, la doctrina estima que, para que se pudiese apreciar este tipo cualificado, haría falta además que el funcionario o autoridad en cuestión los hubiese **cometido sin que mediase causa por delito**.Si lo hiciera actuando dentro y al amparo de una investigación por delito, pero de forma que **superase los límites establecidos**, se habría de **castigar al funcionario conforme a lo establecido en los delitos de los artículos 535 y 536 CP y no atendiendo a lo que define el tipo cualificado del art. 198 CP**. Así sucedería, por ejemplo, cuando el funcionario en cuestión hubiese prolongado una interceptación de comunicaciones realizada al amparo de una investigación por delito más allá de lo que se le había autorizado judicialmente o la hubiese extendido a terminales no incluidos en su autorización.

En el presente caso, dado que desconocemos tanto las fechas de origen y de final de las infecciones no podemos afirmar ni negar la existencia de una causa judicial por delito que pudiera amparar a los querellados, pero lo que es evidente es que uno de los dos delitos sí ha sido cometido. Solo la progresiva cristalización de la instrucción podrá desvelarlo.

Cuarto- De la agravante de comisión del delito en el seno de un grupo criminal (Art. 197 quater)

A la hora de caracterizar al **grupo criminal,** señala la STS 216/2018 de 8 May. 2018, que no se trata de una "*unión fortuita para la comisión inmediata de un solo delito*", sino que los grupos criminales, definidos en el art. 570ter CP precisamente por exclusión, es decir, como formas de concertación criminal que no encajan en el arquetipo de la organización criminal, pero sí aportan un plus de peligrosidad criminal a las acciones de sus componentes". "*La estructura de las nuevas infracciones -añade la exposición de motivos de la LO 5/2010- responde a un esquema similar en ambos casos,* ***organizaciones*** *y grupos, si bien por un lado las penas son más graves en el caso de las primeras,* ***cuya estructura más compleja responde al deliberado propósito de constituir una amenaza cualitativa y cuantitativamente mayor para la seguridad y orden jurídico****, y por otra parte su distinta naturaleza exige algunas diferencias en la descripción de las acciones típicas".*

El concepto de **grupo criminal** es, pues, **de carácter residual frente al de organización criminal**, con el que presenta algunas semejanzas, como el hecho de estar constituido por la **unión de más de dos personas y tener por finalidad la perpetración concertada de delitos**; sin embargo, se crea sobre los conceptos negativos de no concurrencia de alguna o algunas de las características de la organización criminal, de modo que basta la no concurrencia de uno de los elementos estructurales del tipo de organización delictiva, para que surja la figura de grupo criminal.

En definitiva y a tenor de la anterior **definición legal el grupo criminal sólo requiere de dos elementos**:

a.- **Pluralidad subjetiva**: unión de **más de dos personas**.

b.- **Finalidad criminal**: pues debe tener por finalidad u objeto la perpetración concertada de delitos.

c.- El **grupo deberá presentar una cierta estabilidad, aunque sea menor** a la exigida para la organización criminal, lo que permitiría apreciar su existencia aun cuando su formación tenga por objeto la comisión de un solo delito, siempre que esté presente una cierta complejidad y una exigencia de mantenimiento temporal

relevante, que vendría a permitir nuevos delitos similares.

El precepto **no incluye como elemento del tipo objetivo, ni el contacto personal entre los integrantes del grupo ni la presencia necesaria de todos y cada uno de los integrantes del grupo en todas y cada de las infracciones que al mismo se atribuyan**. La concertación a que se refiere aquel precepto no evoca, ni siquiera en su significado genuinamente gramatical, la proximidad física entre aquellos que se conciertan. Dicho de forma más gráfica, el acuerdo de voluntades y la asunción de cometidos pueden realizarse a distancia, sin necesidad de compartir el mismo escenario. Es más, no son descartables los casos en los que esa falta de conocimiento personal entre quienes delinquen concertados sea la consecuencia de una elemental estrategia delictiva orientada a evitar la delación.

SÉPTIMO.- DE LA ADMISIÓN A TRÁMITE E INVESTIGACIÓN DE ESTA QUERELLA.

Se han aportado indicios suficientes, en este momento inicial, para abrir una investigación penal por los hechos relatados.

Es evidente que los querellantes NO pueden aportar una acreditación detallada y ya cristalizada de todos los hechos denunciados, especialmente dada la complejidad de estos (Delitos informáticos a través de software específicamente diseñado para ocultar su trazabilidad, cometidos parcialmente en el extranjero por empresas completamente inaccesibles, y contratadas por autoridades de inteligencia amparadas por las Leyes de Secretos de Estado y de Fondos Reservados), más no es esa su función sino simplemente la de poner estos hechos indiciariamente delictivos en conocimiento de las autoridades.

En relación con el *ius ut procedatur*, la STC 141/2011, de 26 de septiembre, FJ 4, con mención de otras muchas resoluciones que se pronuncian en el mismo sentido, recuerda la clásica doctrina que:

"Lo que en realidad implica este principio es la interdicción de aquellas decisiones de inadmisión –o de no pronunciamiento– que por su rigorismo, por su formalismo excesivo o por cualquier otra razón revelen una clara desproporción entre los fines que aquellas causas de inadmisión –o no pronunciamiento sobre el fondo– preservan y los intereses que sacrifican".

Como dice la STS 5817/2013, de 04 de diciembre: "En efecto, la pretensión de que desde el mismo acto judicial de incoación del procedimiento instructor queden perfectamente definidos los hechos sometidos a investigación, e incluso las calificaciones jurídicas de los delitos que pudieran constituir tales hechos, no es aceptable. La ley podría establecerlo así, impidiendo que los Juzgados de Instrucción instruyeran causas que no fueran planteadas mediante querella; pero lo cierto es que la ley vigente permite incoar diligencias a partir de una mera denuncia, y tanto uno como otro de estos sistemas es compatible con los derechos del art. 24 C.E. (SSTC 173/1987, 145/1988 , 186/1990 , 32/1994). ***Sólo cuando los hechos van siendo esclarecidos, en el curso de la investigación, es posible, y exigible, que la acusación quede claramente perfilada, tanto fáctica como jurídicamente*** *(SSTC 135/1989 , y 41/1997).*

El ATS de 15 de julio de 2009, Recurso 20048/2009, que nos indica que: *"La iniciación del proceso no es consecuente a la responsabilidad penal, sino la previa condición, esto es, el presupuesto imprescindible para la averiguación, comprobación y determinación, con las debidas garantías, de la responsabilidad criminal. No se inicia un proceso porque se sea responsable de un delito, sino para poder determinar con garantías si se es o no responsable."*

Y el muy reciente Auto 1984/2024, de 29/05, de la Audiencia Provincial de Madrid señala muy acertada y claramente que debe abrirse investigación, toda vez que:

> *"El artículo 269 de la Ley de Enjuiciamiento Criminal establece que, formalizada que sea la denuncia se procederá o mandará proceder inmediatamente por el Juez o funcionario a quién se hiciese a la comprobación del hecho denunciado,*

salvo que éste no revistiere carácter de delito, o que la denuncia fuera manifiestamente falsa.

[...]

Para la fijación del estándar requerido en cada caso es de utilidad la distinción entre probabilidad, concepto graduable, y posibilidad que hace referencia a dos alternativas incompatibles (posible/imposible). Así, en la decisión inicial de admitir a trámite una denuncia o querella bastará una posibilidad cierta basada en datos objetivos.

Para la admisión de la denuncia basta la verosimilitud, la mera posibilidad fundada, muy alejada de los indicios racionales suficientes de criminalidad que sirven para el procesamiento o prosecución por los trámites del procedimiento abreviado, e incluso de los simples indicios para llamar ya a una persona a declarar como investigada. Lo contrario llevaría al absurdo de solo poder incoar diligencias de investigación por hechos que contengan no sólo la descripción de una conducta susceptible de tener relevancia penal, sino una alta probabilidad de condena lo que distorsionaría la función investigadora de esta fase inicial del proceso, anterior a la inculpación judicial. De ahí que el legislador pretendiera restar carga estigmatizadora a la condición de mero investigado suprimiendo la condición de imputado.

La pretensión del Ministerio Fiscal de impedir toda investigación amparándose en una taxativa interpretación típica, ab initio, en este delicado campo es inusual y podría llevar a crear lagunas de impunidad en toda actividad delictiva donde la delimitación del comportamiento penalmente relevante no siempre es fácil de establecer, y donde la obtención de fuentes de prueba es compleja. El fin y las garantías del procedimiento están diseñadas en sentido contrario. ***Al inicio debe bastar, como venimos repitiendo, una sospecha fundada en datos objetivos y verificables, que tendrá que ir decantándose y superando los filtros establecidos*** *para, en su caso, llamar a alguien a declarar como investigada, posteriormente*

acordar la continuación del procedimiento, y finalmente poder condenar. Si, por el contrario, verificadas las comprobaciones e investigaciones precisas la hipótesis se diluye procederá acordar el archivo inmediato.

[...] el Tribunal Constitucional exige para la incoación de un procedimiento, exigiendo en lo que respecta a los indicios, que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento. Esto es, "sospechas fundadas" en alguna clase de datos objetivos, que han de serlo en un doble sentido: en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona, citándose las SSTC 49/1999; 166/1999; 171/1999; 299/2000."

Particularmente representativo es el Auto de 06/11/2023 del Juzgado Central de Instrucción 6:

"Como señala el Auto del TS, Sala Segunda, de 31/10/2017 (CAUSA ESPECIAL/20907/2017, Ponente D. Manuel Marchena) "...el objeto del proceso penal es de cristalización progresiva. Se dibuja de una forma incipiente con la denuncia o querella y se va formateando conforme avanzan las investigaciones. Será a lo largo de la instrucción cuando los hechos imputados, a la vista de las diligencias de investigación acordadas por el instructor, confirmen o desmientan su realidad. Y será entonces cuando pueda precisarse la calificación.

[...]

Así, es doctrina Jurisprudencial asentada (STS 908/2021, 521/2015, 228/2013, entre otras) que no es aceptable "la pretensión de que desde el mismo acto judicial de incoación del procedimiento instructor queden perfectamente definidos los hechos sometidos a investigación, e incluso las calificaciones jurídicas de los delitos que pudieran constituir tales hechos". Y es que, en efecto

la ley podría establecerlo así, impidiendo que los Juzgados de Instrucción instruyeran causas que no fueran planteadas mediante querellas en que quien ejerce la acusación delimite perfectamente desde el inicio todos los extremos de la investigación; pero lo cierto es que también es doctrina constitucional consolidada (SSTC 173/1987, 145/1988, 186/1990, 32/199) que la ley vigente permite incoar diligencias a partir de una mera denuncia, y tanto uno como otro de estos sistemas es compatible con los derechos del art. 24 CE, y que, sólo cuando los hechos van siendo esclarecidos, en el curso de la investigación, es posible, y exigible, que la acusación quede claramente perfilada, tanto fáctica como jurídicamente (SSTC 135/1989 y 41/1997).

La finalidad a que ha de tender toda instrucción criminal es, en consecuencia la de la delimitación progresiva del objeto del proceso buscando averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en la calificación y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos (art. 299 LECrim), y que acabará en el auto de procesamiento (o de Apertura del Procedimiento Penal) donde el Magistrado instructor "exterioriza los indicios de criminalidad que la investigación ha podido poner de manifiesto y se sientan los presupuestos fácticos a partir de los cuales resolver interinamente los problemas de conexidad" (Auto Sala Segunda 27/12/2018, Causa Especial 20907/2017).

OCTAVO.- DILIGENCIAS QUE SE INTERESAN.

A la luz de lo anterior, solicitamos de este Juzgado Central la práctica d elas siguientes Diligencias de investigación.

1.- Declaración de los querellantes.

2.- Interrogatorio de los querellados.

3.- Se requiera a los Mossos d'Esquadra a fin de que realicen sobre los

dispositivos electrónicos de mis representados que éstos entregrarán cuando sean requeridos para ello **el correspondiente informe pericial informático que acredite la utilización del spyware Candiru y/o Pegasus sobre los mismos, detallando las fechas de intento de infección, las fechas de infección exitosas, y todas las coordenadas informáticas que permitan identificar la forma de acceso, cantidad y calidad de los datos accedios y extraídos y posibles autores de los mismos.**

4.- Declaración pericial de los autores de los dos informes de The Citizen Lab "*Catalangate, Extensive mercenary spyware operation against Catalans using Pegasus and Candiru*" y "*Hooking Candiru, another mercenary spyware vendor comes into focus*", quienes son:

- Bill Marczake,
- John Scott-Railton,
- Kristin Berdan,
- Bahr Abdul Razzak,
- Sienna Anstis,
- Gözde Böcü,
- Salvatore Solimano
- Ron Deibert.

5.- Declaración pericial de los autores del informe de Forensic Architecture de Amnesty International que han corroborado digitalmente las infecciones recogidas por The Citizen Lab.

6.- Se solicite al Punto Neutro Judicial que recabe toda la información posible

en España de todos los querellados que no tengan domicilio en España, esto es todos, salvo Dña. Paz Esteban López; D. Feliz Vicente Azón Vilas y Dña. María Gámez Gámez.

7.- Se libre exhorto al Juzgado Central de Instrucción 6 a fin de que remita copia testimoniada de la Pieza Separada 1 de las DDPP 85/2019 (Registro General 348/19) en la que mis representados fueron objeto de investigación por la Guardia Civil bajo la dirección de dicho Juzgado, sinque cristalizara en ninguna acusación formal.

8.- Se libre exhorto al Juzgado Central de Instrucción 6 a fin de que remita copia testimoniada de la parte de las DDPP 99/2018 (Causa Judas) y todas sus eventuales piezas separadas, que estén relacionadas o afecten al protocolo de voto electrónioco Vocdoni, cuyo desarrollo informático corrió a cargo de varios de mis representados.

9.- Se libre Orden Europea de Investigación al Gran Ducado de Luxemburgo, al amparo del Título X de la Ley 23/2014, a fn de que las autoridades luxemburguesas competentes lleven a cabo las siguientes medidas de investigación respecto de los siguientes: **OSY TECHNOLOGIES Sarl; Q CYBER TECHNOLOGIES Sarl, Shalev Hulio, Omri Lavie y Yuval Somekh.**

- Les tomen declaración en calidad de investigados.

- Requieran a los querellados a fin de que manifiesten si han suscrito, por sí o a través de empresas que controlen directa o indirectamente, convenios o contratos de cualquier tipo con las autoridades españolas y aporten copia de los mismos.

- Requieran a los querellados a fin de que entreguen toda documentación, de cualquier clase o función y en cualquier formato, que hayan cruzado, por sí o a través de empresas que controlen directa o indirectamente, con autoridades españolas, hayan suscrito con autoridades españolas o hayan

recibido de autoridades españolas.

- Faciliten relación de las transferencias bancarias que las dos empresas citadas, por sí o a través de empresas que controlen directa o indirectamente, hayan podido enviar o recibir de cualesquiera autoridades españolas desde el 2.018 hasta la actualidad.

10.- Se libre comisión rogatoria internacional al Estado de Israel, a fin de que las autoridades israelíes competentes realicen las siguientes medidas de investigación respecto de los siguientes: **NSO GROUP TECHNOLOGIES Ltd, Q CYBER TECHNOLOGIES Ltd; SAITO TECH Ltd, Eran Shorer, Ya'akov Weizman y Eitan Achlow:**

- Les tomen declaración en calidad de investigados.

- Requieran a los querellados a fin de que manifiesten si han suscrito, por sí o a través de empresas que controlen directa o indirectamente, convenios o contratos de cualquier tipo con las autoridades españolas y aporten copia de los mismos.

- Requieran a los querellados a fin de que entreguen toda documentación, de cualquier clase o función y en cualquier formato, suya o de empresas que controlen directa o indirectamente,que hayan cruzado con autoridades españolas, hayan suscrito con autoridades españolas o hayan recibido de autoridades españolas.

- Faciliten relación de las transferencias bancarias que las tres empresas citadas, por sí o a través de empresas que controlen directa o indirectamente, hayan podido enviar o recibir de cualesquiera autoridades españolas desde el 2.018 hasta la actualidad.

11.- Eleve exposición razonada al Consejo de Ministros, por conducto del Ministro del Interior y de conformidad con lo previsto en los artículos 4 y 7 de la Ley 9/1968, de 5 de abril, sobre secretos oficiales, **solicite la desclasificación, para su unión a estas actuaciones, de toda la documentación disponible sobre los querellantes que verse sobre la instalación del software Candiru o Pegasus por cualesquiera autoridad, agencia o administración del Gobierno Español que haya permitido a ésta, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de sus terminales, aportando las decisiones administrativas o, en su caso judiciales, que habilitaron dichas instalaciones de software espía, los expedientes administrativos de cada una de estas medidas de investigación y toda la documentación generada u obtenida durante la vida de las medidas, así como el coste de dicho proceso de instalación y análisis y las partidas presupuestarias específicas en que fueron subsumidos dichos costes.**

12.- Libre atento oficio al Consejo de Ministros, a fin de que éste conceda la correspondiente dispensa a los querellados Paz Esteban López, Felix Vicente Azón Vilas y María Gámez Gámez relativas a sus declaraciones ante este Juzgado que versen sobre la instalación de software Candiru o Pegasus por cualesquiera autoridad, agencia o administración del Gobierno Español que haya permitido a ésta, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de sus terminales, aportando las decisiones administrativas o, en su caso judiciales, que habilitaron dichas instalaciones de software espía, los expedientes administrativos de cada una de estas medidas de investigación y toda la documentación generada u obtenida durante la vida de las medidas, así como el coste de dicho proceso de instalación y análisis y las partidas presupuestarias específicas en que fueron subsumidos dichos costes.

En virtud de lo anterior,

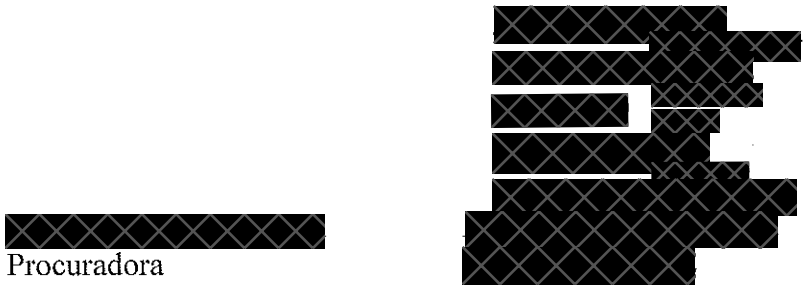
AL JUZGADO SOLICITO que, teniendo por presentado este escrito junto con su documentación adjunta, se sirva admitirla y tenga por presentada **QUERELLA en nombre de las víctimas enumeradas en el Apartado Segundo y contra las personas y mercantiles enumeradas en el Apartado Tercero, acordando practicar las diligencias de investigación señaladas en nuestro Apartado Octavo.**

Es todo ello Justicia que pido en Barcelona, a 29 de abril de 2025.

OTROSÍ DIGO que, habiendo presentado poderes apud acta electrónicos que no recogen todos los extremos señalados por el art. 277 LECrim, por no existir dicha posibilidad en la sede judicial electrónica de la Administración de Justicia, solicito la citación de nuestros representados para ratificar los mismos.

AL JUZGADO SOLICITO que tenga por hechas las manifestaciones anteriores y por solicitada la ratificación de los poderes especiales apud acta aportados con esta querella.

Es Justicia que pido en fecha y lugar ut supra señalados.



Procuradora