

Agencia Vasca de Protección de Datos con copia para Agencia Española de Protección de Datos AEPD Atn. Mar España Martí y Olga Pérez Sanjuán Defensor del Pueblo Prof. Dr. Ángel Gabilondo, Ministra de Defensa Margarita Robles y a quien pudiera interesar esta **DENUNCIA publicada en <https://www.miguelgallardo.es/espionaje-vasco.pdf>**

Estamos investigando y denunciando usos indebidos de tecnologías intrusivas como el sistema spyware [PEGASUS](#) de NSO Group, los interceptadores o IMSI Catchers o StingRays como [VERINT](#) y los clonadores de teléfonos móviles SMARTPHONES conocidos como [CELLEBRITE](#) (UFED). En los archivos y registros de la Agencia Española de Protección de Datos AEPD constan numerosos escritos nuestros en relación a esos sistemas intrusivos que no deben ser empleados sin una bien motivada y precisa orden judicial “ad hoc”. Las tecnologías para espiar teléfonos móviles SMARTPHONES en toda Europa deben estar celosamente controladas, garantizando la seguridad jurídica y la interdicción de la arbitrariedad en las intrusiones. La transparencia no solamente no es contraria a la Seguridad de un Estado, sino que es imprescindible para proteger eficazmente el interés general ciudadano.

La mera posibilidad de que esos sistemas ([PEGASUS](#), [VERINT](#) o [CELLEBRITE](#)), u otros asemejables, puedan ser utilizados por gobiernos autonómicos, o municipales, o cualquier entidad pública, y más aún si es privada, nos motiva para presentar denuncias, al menos, hasta que un funcionario responsable y competente, nos informe y actúe de oficio. En este sentido, aquí **denunciamos lo que puede verse publicado en <https://www.elsaltodiario.com/espionaje/contrato-secreto-gobierno-vasco-batalla-firmas-israel-caso-pegasus> que hemos preservado en <https://cita.es/pegasus-vasco.pdf>**

*Un contrato “secreto” del Gobierno Vasco desata una batalla entre dos firmas conectadas al caso Pegasus Mientras el PNV exige en Madrid desclasificar documentos de la trama de espionaje Pegasus, el Gobierno Vasco declara “secreto por razones de seguridad” el expediente para la “evolución del sistema de intervención legal de comunicaciones de la Ertzaintza”. Las dos licitadoras enfrentadas son distribuidoras de la empresa que ha diseñado el programa de espionaje israelí, entre ellas, la de una familia muy cercana a Benjamin Netanyahu. Ahoztar Zelaieta @Ahoztar1972 (<https://twitter.com/Ahoztar1972>) 30 MAY 2022 05:44 El pasado jueves, subido a la tribuna del Congreso de los Diputados, Aitor Esteban ([https://www.youtube.com/watch?v=JcNKFTpgmx4&feature=youtu.be&ab\\_channel=PedroVallin](https://www.youtube.com/watch?v=JcNKFTpgmx4&feature=youtu.be&ab_channel=PedroVallin)) afirmaba que “un cierre en falso del caso Pegasus” no ayudaría “a la mejora del sistema democrático” e indicaba que sería más “propio” pluralizar y “hablar de los espionajes”. Días antes, Aitor Esteban señalaba que “nadie tiene certeza de no ser espiado” y exigía a Pedro Sánchez desclasificar documentos. Como ha podido saber Hordago-El Salto gracias a una resolución del Órgano Administrativo de Recursos Contractuales de Euskadi de finales de marzo, mientras el portavoz del PNV vende consejos en Madrid, el Gobierno vasco oculta su relación con las empresas israelíes que facilitan el espionaje a la Ertzaintza. A este respecto, la Plataforma de Contratación Pública de Euskadi oculta la licitación de un contrato para la “evolución del sistema de intervención legal de comunicaciones de la Ertzaintza”. Según fuentes de Seguridad del Estado citadas por El Periódico, las dos empresas (Excem y Dars Telecom) que pujaban por la adjudicación son intermediarias de NSO Group, firma israelí que ha desarrollado el programa Pegasus. Tal vez por este motivo, el expediente ha sido declarado “secreto” por parte del Ejecutivo de Iñigo Urkullu alegando “razones de seguridad”. Pegasus inquieta al PNV Hace casi un año, en julio del 2020, se destapó un escándalo mundial al publicarse*

(<https://www.theguardian.com/world/2021/jul/18/revealed-leakuncovers-global-abuse-of-cyber-surveillance-weapons-group-pegasus>) que el programa Pegasus había espiado a líderes de todo el planeta, incluyendo a los independentistas catalanes. El hecho de que la empresa involucrada fuera la firma israelí NSO Group puso en jaque los planes de la Consejería de Seguridad del Gobierno Vasco. Meses después, a principios de 2021, la Ertzaintza reaccionó cambiando sus planes para adjudicar el sistema de intervención de comunicaciones licitado bajo el nombre de “Evolución del sistema de comunicaciones, licitado bajo el nombre de Evolución del sistema de intervención legal de comunicaciones de la Ertzaintza”. Este sistema ha sido fabricado por Verint Systems, una firma israelí de inteligencia que en 2018 trató de comprar NSO Group. Hasta el momento, la gestión del servicio había recaído en Excem Grupo 1971 SA, proveedora en el Estado español de Verint, así como proveedora tecnológica de la “policía patriótica” del PP y del Ministerio de Defensa. Excem es de la familia Hatchwell, muy cercana a Benjamin Netanyahu, como publicó El Confidencial ([https://www.elconfidencial.com/eleccionesgenerales/2016-06-24/oac-grabaciones-espionaje-cintas-interior-fernandezdiaz\\_1222177/](https://www.elconfidencial.com/eleccionesgenerales/2016-06-24/oac-grabaciones-espionaje-cintas-interior-fernandezdiaz_1222177/)). En poco menos de un año, la sangre ha llegado al río y salpica al partido jeltzale de Aitor Esteban. El 5 de enero de 2022, Excem presentaba un recurso especial contra la adjudicación del citado contrato en el registro del Órgano Administrativo de Recursos Contractuales de la Comunidad Autónoma de Euskadi (OARC). El representante español de la israelí Verint Systems había perdido la nueva adjudicación tras casi dos décadas como proveedora. En su lugar, la licitación fue entregada a la firma italo-española Dars Telecom SL, intermediaria también de la firma israelí NSO Group, fabricante del software de espionaje Pegasus. Por ello, surgen algunas preguntas: ¿hasta qué punto las empresas de inteligencia de este país han penetrado en la policía vasca y el Ejecutivo vasco como para provocar conflictos internos entre ambas? Si se tratara de un contrato normal, el Gobierno Vasco no hubiera protegido con tanto ahínco los entresijos de este. Entonces, ¿por qué imploró a la OARC que guardara silencio?. “Al tratarse de un expediente declarado secreto por razones de seguridad, [debe garantizarse] de la manera más estricta posible la confidencialidad y el secreto de la información,” señala el Gobierno Vasco en sus alegaciones al OARC. Irregularidades en el Gobierno Vasco Ahora bien, no se trata de un expediente cualquiera, sino de un expediente considerado como ilegal por la empresa demandante, con quien el PNV ha mantenido buenas relaciones hasta que estalló el escándalo Pegasus. En su recurso Excem alega que una resolución del Gobierno Vasco acordó en recurso, Excem alega que una resolución del Gobierno Vasco acordó en septiembre de 2021 abrir una nueva fase de negociación acotando las necesidades mínimas y los valores máximos valorables. Para ello, había solicitado a las dos empresas una nueva oferta económica definitiva que no estaba prevista en los pliegos de la licitación, “lo que supone una infracción del procedimiento legalmente establecido”. Según Excem, además, “se da la circunstancia de que, con anterioridad a dicha resolución, ya había ofertas definitivas” y la suya “era la mejor puntuada” en junio de 2021. Dars Telecom solicitó la desestimación del recurso al entender que la solicitud de Excem “carece de argumentación jurídica sobre el fondo del asunto y perjudica al interés público por tratar de entorpecer la formalización del contrato”. ¿Por qué cambió de idea a última hora, contradiciendo además los criterios de la ley de contratación? Por su parte, el Gobierno Vasco señaló al organismo regulador que una cláusula especial de los pliegos de la licitación “no ha establecido ni limitado el número de fases o rondas de negociación”. Pero a juicio del OARC, “en este caso el poder adjudicador ha infringido el procedimiento legalmente aplicable”. El motivo: “solicitar la modificación de ofertas ya recibidas” que el propio Gobierno Vasco había considerado como “definitivas y, consecuentemente, innegociables”, para “elevar la propuesta al órgano de contratación” que adjudicaría el contrato. Este movimiento del Gobierno Vasco ha llevado al Órgano Administrativo de Recursos Contractuales de la Comunidad Autónoma de Euskadi (OARC) a acusarle de “alterar un criterio de adjudicación por introducir en él un umbral máximo que no figuraba originalmente en su descripción”. Esto es, el Gobierno Vasco se ha saltado la normativa de contratación para no adjudicar un contrato a una proveedora israelí con la que llevaba varios años trabajando y entregárselo a otra cuya identidad conocía. El 25 de marzo de 2022, el OARC ha terminado estimando “parcialmente” el recurso de Excem. Según esta firma, la otra licitadora, Dars Telecom, llegó a introducir “en el sobre de los criterios de adjudicación sujetos a juicio de valor” datos que no debía incluir, como su identidad, ya que “anticipan información” y ello suponía “un intento de influir en la objetividad del juicio del evaluador y comprometer el secreto de la proposición”. Aunque el OARC decretó “levantar la suspensión del procedimiento de adjudicación”, la Plataforma de Contratación Pública de Euskadi sigue sin publicar ni un solo dato sobre el proceso de licitación y adjudicación. Trío de intermediarios Este 21 de mayo, Hordago-EI Salto desveló las relaciones de Verint Systems con el Gobierno Vasco, adjudicataria en 2003 del Sistema de Monitorización Telefónica de la Ertzaintza. La investigación apunta que la firma española Excem “presta sus servicios de soporte y mantenimiento así como el suministro de componentes y materiales precisos para el funcionamiento” del Sistema de Intervención Legal de Comunicaciones de la Ertzaintza. Así fue desde el año 2006, cuando Excem era el “único y exclusivo representante en el Estado español” de la israelí Verint Systems. Por entonces, Julián García Vargas, exministro de Defensa, era consejero delegado de Excem. No obstante, el reportaje destapaba también que eso había cambiado y el contrato citado en la sección anterior para la “evolución del sistema de intervención legal de comunicaciones de la Ertzaintza” fue adjudicado a Dars Telecom. Seis horas después, el diario catalán El Periódico (<https://www.elperiodico.com/es/politica/20220521/espionaje-aragones-costos-43000-euros-cni-pegasus-13687730>), citando fuentes de Seguridad del Estado, afirmaba que Dars Telecom y Excem son intermediarias de la también israelí NSO Group para la distribución de su spyware denominado Pegasus. Entre los directivos de Dars Telecom citados por El Periódico destacan Michele Tomba y Alberto Chiappino, ambos mencionados en la filtración de WikiLeaks (<https://wikileaks.org/hackingteam/emails/emailid/9207>), debido a su conexión con la trama de espionaje de la firma italiana Hacking Team. Esta última había sido contratada por el CNI

([https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos\\_916216/](https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/)) para espiar teléfonos móviles y ha sido cliente de la Ertzaintza (<https://gananzia.com/la-ertzaintza-yempresas-vascas-figuran-entre-los-supuestos-clientes-de-la-firma-de-espionaje-online-hacking-team>) En los datos de WikiLeaks figura también que el socio 29/8/22, 14:32 Espionaje | Un contrato “secreto” del Gobierno Vasco desata una batalla entre dos firmas conectadas online hacking team). En los datos de WikiLeaks figura también que el socio local de Hacking Team es Galea Electricuna empresa vasca manejada por la familia responsable de la obra del edificio del Archivo Histórico del Nacionalismo de Artea. Entonces, ¿las irregularidades del Gobierno Vasco se deben al caso Pegasus o al choque de intereses entre las firmas israelíes, quienes llevan décadas compitiendo y enfrentándose por los contratos de espionaje de las Fuerzas de Seguridad del Estado, incluyendo a la Ertzaintza? Las amistades de Dars Telecom La relación de Dars Telecom con las Fuerzas de Seguridad del Estado va más allá que sus relaciones mercantiles con la Ertzaintza. Esta firma ha sido proveedora tanto del Gobierno Vasco como de la Policía patriótica del PP que, según Aitor Esteban, le habría habria espiado (<https://www.lavanguardia.com/politica/20220425/8220351/aitor-pnv-estebanmas-absoluta-certeza-telefono-pinchado-mocion-censura-rajoy.html>) durante la moción de censura contra Mariano Rajoy. Aquello ocurrió meses después de dirigirle la famosa frase de “si bien me quieres, Mariano, da menos leña y más grano”. Según los datos hechos públicos entre los años 2015 (<https://www.boe.es/boe/dias/2015/06/19/pdfs/BOE-B-2015-19743.pdf>) y 2021, ([https://contrataciondelestado.es/wps/wcm/connect/2e265b22-9cfa-49d9-b4e7-8de3284640f2/DOC\\_FORM2021-317581.html?MOD=AJPERES](https://contrataciondelestado.es/wps/wcm/connect/2e265b22-9cfa-49d9-b4e7-8de3284640f2/DOC_FORM2021-317581.html?MOD=AJPERES)) a los que ha tenido acceso Hordago-El Salto, Dars Telecom ha sido adjudicataria de importantes contratos de suministro de equipos y software para la interceptación de las telecomunicaciones utilizados por el Cuerpo Nacional de Policía y la Guardia Civil. Según la Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio (TEDAE), la firma italo-española también trabaja para el Ministerio de Defensa y la Policía Foral navarra. De acuerdo al TEDAE, entre los productos ofertados por Dars Telecom se incluyen los “centros de monitorización, soluciones específicas de interceptación legal para los operadores herramientas de investigación en distintos entornos los operadores, herramientas de investigación en distintos entornos tecnológicos avanzados como pueden ser redes sociales, TOR, balizas electrónicas y soluciones para la gestión electrónica de mandamientos judiciales en conservación de datos, intervenciones telefónicas y oficios policiales tanto para operadores de comunicaciones como para cuerpos y fuerza de seguridad”. Dars Telecom fue adquirida en diciembre del 2021 por la empresa Cy4gate. La plataforma que investigó el espionaje a independentistas con el programa Pegasus, Citizen Lab, desveló que Cy4gate estaba implicada en la distribución de una versión falsa (<https://imagenpoblana.com/21/02/04/alerta-sobre-falsaversion-de-whatsapp-que-roba-datos-personales>) de la aplicación de mensajería WhatsApp utilizada para robar información. Espionaje “made in Italy El Periódico también informaba el pasado 21 de mayo sobre Roberto Raffelli, presidente de Dars Telecom entre 2006 y 2010 y patrón de la firma italiana RCS Lab. Esta última fue contratista de la Fiscalía de Italia hasta 2015, fecha en la que Roberto Raffelli fue “acusado de pasar grabaciones obtenidas a través de la fiscalía al presidente italiano Silvio Berlusconi”. Cabe señalar que el desembarco de Silvio Berlusconi en el sector televisivo español se produjo en 1988 gracias a un convenio firmado con el ente público vasco ETB. Poco después, un testaferro de Berlusconi, Donaldo Nicosia, comenzó a tejer una red de empresas en Euskadi, gran parte de ellas domiciliadas en la sede de una gestoría propiedad del hermano de un exresponsable de las finanzas del PNV. Esta gestoría estuvo ligada al affaire del caso Tragaperras, sobre supuesta financiación ilegal del PNV, y Donaldo Nicosia figura en los papeles de Panamá a través de una empresa con sede en Bilbao. No son estas las únicas relaciones del Gobierno Vasco con contratistas italianos del Ministerio de Defensa como Dars Telecom y Hacking Team. En la década de los años 80, la empresa italiana Telettra, proveedora del Ejército español y de la que fue presidente el exministro de Defensa Eduardo Serra, suministró e instaló las antenas parabólicas del sistema de comunicaciones del Departamento de Interior. ‘El Padrino’ de Aitor Esteban Aitor Esteban señalaba hace algunos días que al PNV le “han espiado toda la vida y lo van a seguir haciendo”. El Portavoz del Grupo Vasco en el Congreso de los Diputados, evitaba hacer autocritica de los episodios de espionaje ligados a la Ertzaintza, desde el caso de las escuchas al exlehendakari Carlos Garaikoetxea hasta el caso Tellería. De hecho, el sistema de monitorización telefónica de la Ertzaintza no ha estado siempre en manos de empresas extranjeras. Antes de encargar el sistema a la empresa israelí Verint Systems en 2003, el Gobierno Vasco contrataba a Telion SA, una empresa vasca de confianza, para ese servicio de mantenimiento del Sistema de Monitorización Telefónica de la Ertzaintza. Telion estaba por entonces controlada por Dominion y Urazca, ambas vinculadas a importantes apellidos del PNV, y había crecido como una importante contratista de ETB. Entre 1999 y 2004, la presidencia de Dominion la ostentó Abel Matutes, alcalde de Ibiza durante la dictadura franquista, ministro de Asuntos Exteriores del primer gabinete de José María Aznar que tenía el apoyo del PNV, exsocio de empresarios vascos en el negocio de las discotecas y con intereses en Panamá. A partir de 2004, Dominion pasó a estar presidida por Antón Pradera, consejero de la firma desde 1999 y hermano del jeltzale José Alberto Pradera, exDiputado General de Bizkaia cuyo nombre figura en los papeles de Panamá. Por su parte, Urazca era propiedad de Javier Uría, exalcalde de Zeberio y figura de la élite vasca que apadrinó las carreras políticas de Itxaso Atutxa, presidenta del Bizkai Buru Batzar, y Aitor Esteban, portavoz del PNV en el Congreso. Urazca, empresa fundada por su padrino político, figura en los papeles de Bárcenas y en la trama de comisiones ilegales de burukides del PNV denominada caso De Miguel.

Por lo expuesto, como mejor proceda, **SOLICITAMOS**:

1º Que se requiera al Gobierno Vasco todo cuanto conste en sus archivos y registros relativos a **PEGASUS**, **VERINT** o **CELLEBRITE** u otros asemejables precisando qué equipos han estado operativos y cuáles lo están actualmente.

2º Que se identifiquen a todos los funcionarios que tienen acceso a sistemas intrusivos en el Gobierno Vasco.

3º Que se promueva la máxima transparencia posible sobre las tecnologías intrusivas como **PEGASUS**, **VERINT** o **CELLEBRITE** u otros asemejables con los únicos límites que pudieran afectar a la Seguridad Nacional (que no puede ser la misma que la autonómica) y a los datos y metadatos personales de los particulares afectados, tanto por las intrusiones en un teléfono, como por haber estado en comunicación con alguno intervenido, o incluso por haber sido meramente mencionados o afectados, pero sin haber participado en ninguna conversación intervenida.

4º Que se publique una guía de los derechos que los ciudadanos podemos ejercer respecto a las autoridades y las administraciones que utilizan, más aún si ocultan haber utilizado, sistemas intrusivos como los descritos en <https://www.elsaltodiario.com/espionaje/contrato-secreto-gobierno-vasco-batalla-firmas-israel-caso-pegasus> que hemos preservado en <https://cita.es/pegasus-vasco.pdf>

**OTROSÍ 1** digo que en caso de archivo o de alguna denegación de lo solicitado en esta denuncia, se nos notifique una resolución motivada con pie de recurso, a la mayor brevedad posible.

**OTROSI 2** digo que como denunciantes estamos a la disposición de todos los funcionarios competentes para cualquier explicación o referencia a nuestro alcance, incluso por teléfono, así como para subsanar cualquier defecto que pudiera tener esta denuncia.

Se adjunta otra denuncia anterior ya presentada ante la AEPD que se incluye en este PDF que consta de 8 páginas en total.

[@miguelgallardo](#) Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: [apedanica.ong@gmail.com](mailto:apedanica.ong@gmail.com)

[@APEDANICA](#) Asociación APEDANICA con registro del Ministerio del Interior [www.cita.es/apedanica.pdf](http://www.cita.es/apedanica.pdf)  
<https://cita.es/pegasus-policial> <https://cita.es/pegasus-policial-aepd.pdf>

**Agencia Española de Protección de Datos AEPD Atn. Mar España Martí**

Cc: Defensor del Pueblo Prof. Dr. Ángel Gabilondo Ministra de Defensa Margarita Robles, Ministro de Presidencia Félix Bolaños, Directora de la Agencia Española de Protección de Datos AEPD Mar España Martí, Fiscalía para la Criminalidad Informática Elvira Tejada y Comisiones Parlamentarias competentes sobre esta [DENUNCIA publicada en www.miguelgallardo.es/pegasus-policial.pdf](http://www.miguelgallardo.es/pegasus-policial.pdf)

**Hemos tenido conocimiento de presuntos usos indebidos del sistema Pegasus de la empresa NSO Group que se ha publicado que adquirió de manera irregular el Ministerio del Interior. La noticia más relevante y detallada que hemos encontrado la publicó "El Periódico de España" con fecha 26 de abril del 2022 que se adjunta en PDF y puede verse en <https://cita.es/pegasus-policial-noticia.pdf> en la que leemos todo esto:**

*El empresario israelí Matian Caspy, que según la prensa israelí ejerció de intermediario de la empresa NSO Group, -la propietaria del sistema de espionaje Pegasus-, también suministró a las 'cloacas' de la Policía del Gobierno de Mariano Rajoy un sistema que permitía irrumpir en los teléfonos y dispositivos móviles sin dejar rastro.*

**Los hechos, con datos precisos y un documento muy relevante, deben ser objeto de un expediente, o ampliación del E/06068/2019 que se inició por denuncia de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas [APEDANICA](#), con fecha 19.5.2019, del que reiteramos todo lo ya manifestado que debe constar a la AEPD. No tenemos ninguna referencia de que tan gravísimos hechos ya hayan sido objeto de alguna actuación judicial o administrativa, y tenemos la peor opinión sobre la actitud sospechosamente pasiva de la directora de la AEPD en relación a nuestras denuncias por espionajes ilegales que atentan contra derechos fundamentales, no solamente de quienes utilizan un teléfono ilegalmente intervenido, sino también de quienes se comuniquen con alguno de ellos, e incluso de quienes sean mencionados por los espíados. Todos los números de teléfonos intervenidos por el sistema PEGASUS son víctimas indemnizables, como también lo son quienes se hayan relacionado con esas víctimas, o fueron aludidos. APEDANICA está sopesando varias acciones directas contra todos los que resulten responsables de acciones u omisiones o disfunciones, y aquí advertimos a la (todavía) directora de la AEPD, Mar España Martí, que tomaremos nota de rectificaciones pero denunciaremos a todo el que pretenda censurar hechos y datos de responsables de PEGASUS, así como de todo el que haya obtenido algún beneficio, por indirecto que sea, de algún espionaje. Las víctimas merecen toda protección. Los espías con ánimo de lucro personal, ninguna.**

## Defensor del Pueblo Prof. Dr. Ángel Gabilondo

Cc: Ministra de Defensa Margarita Robles, Ministro de Presidencia Félix Bolaños, Directora de la Agencia Española de Protección de Datos AEPD Mar España Martí, Fiscalía para la Criminalidad Informática Elvira Tejada y Comisiones Parlamentarias competentes por la [queja con solicitudes publicadas en www.cita.es/defensor-pegasus.pdf](http://www.cita.es/defensor-pegasus.pdf)

Desde las primeras noticias sobre el sistema de espionaje PEGASUS de NSO Group, la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas [APEDANICA](http://www.cita.es/apedanica.pdf), con fecha 19.5.2019 se dirigió a la Agencia Española de Protección de Datos AEPD denunciando el **spyware Pegasus de NSO Group** y solicitando que, *a la mayor brevedad, la AEPD abra un expediente para requerir información precisa, completa, detallada y actualizada, al responsable legal de Whatsapp que entendemos que es Facebook, dándonos traslado de cuanto sea relevante para los afectados con especial interés en todo cuanto posibilite ejercer acciones legales contra “ la empresa de ciberseguridad israelí NSO Group ” según puede verse en [www.cita.es/whatsapp-espionaje.pdf](http://www.cita.es/whatsapp-espionaje.pdf)*

**No es admisible que la AEPD eluda su alta responsabilidad** ante los hechos denunciados entonces archivando la denuncia de [APEDANICA](http://www.cita.es/whatsapp-apedanica.pdf) en el expediente E/06068/2019 tal y como puede verse en <http://www.cita.es/whatsapp-aepd-irlanda.pdf>

*Teniendo en cuenta el carácter transfronterizo de la reclamación y dado que WHATSAPP IRELAND LIMITED tiene su establecimiento principal o único en Irlanda, corresponde a la autoridad de protección de datos de ese Estado actuar como autoridad de control principal, a tenor de lo dispuesto en el artículo 56.1 del RGPD. Por ello, de conformidad con el artículo 66 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la Directora de la Agencia Española de Protección de Datos ACUERDA:*  
*PRIMERO: Remitir la reclamación presentada por APEDANICA (ASOCIACIÓN PARA LA PREVENCIÓN Y ESTUDIO DE DELITOS, ABUSOS Y NEGLIGENCIAS EN INFORMÁTICA Y COMUNICACIONES AVANZADAS) a la autoridad de control de Irlanda, a fin de que por la misma se le dé el curso oportuno.*  
*SEGUNDO: Proceder al archivo provisional del procedimiento*

[APEDANICA](http://www.cita.es/apedanica.pdf) ha denunciado, desde 2011, hechos muy graves en Facebook y WhatsApp, pero también en LinkedIn (Microsoft) y la AEPD siempre nos ha dirigido a la autoridad irlandesa sin que nunca recibiéramos respuesta útil alguna. La relativa al espionaje **con datos y referencias precisas sobre PEGASUS y NSO Group** está publicada en <http://www.miguelgallardo.es/helen-dixon/> incluyendo los PDF

## **Helen Dixon, Data Protection Commissioner in Ireland**

Address: Data Protection Commission 21 Fitzwilliam Square South Dublin 2 D02 RD28 Ireland

<https://twitter.com/APEDANICA/status/1303723740375789568>

[Document published at www.cita.es/whatsapp-pegasus-ireland.pdf](http://www.cita.es/whatsapp-pegasus-ireland.pdf)

## **M. H. Sr. Roger Torrent i Ramió President del Parlament de Catalunya por [carta abierta](#) en**

<https://twitter.com/APEDANICA/status/1284433622209122304>

[y publicada en www.cita.es/president-pegasus.pdf](http://www.cita.es/president-pegasus.pdf)

## **Mark Zuckerberg at Facebook (WhatsApp)**

Attn. COOLEY LLP TRAVIS LEBLANC JOSEPH D. MORNIN DANIEL J. GROOMS

[OPEN LETTER published at www.miguelgallardo.es/whatsapp-pegasus.pdf](http://www.miguelgallardo.es/whatsapp-pegasus.pdf)

## **PEGASUS and NSO Group cellular spying**

[Document published at www.cita.es/pegasus.pdf](http://www.cita.es/pegasus.pdf)

## **Palestinian BDS National Committee BNC**

[Document published at www.cita.es/anyvision-palestinians.pdf](http://www.cita.es/anyvision-palestinians.pdf)

Por lo expuesto, como mejor proceda, la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas [APEDANICA](#) presenta esta queja al Defensor del Pueblo contra la Directora de la Agencia Española de Protección de Datos AEPD Mar España Martí y solicita:

1º Que se requiera a la AEDP todo cuanto conste en sus archivos y registros relativos a PEGASUS y además, se le inste a solicitar a la autoridad de control de Irlanda todo cuanto pueda ser relevante, proponiendo y estableciendo un protocolo que asegure que la AEPD ofrece a los españoles tanta información como tengan los irlandeses.

2º Que el Defensor del Pueblo promueva la coordinación entre instituciones semejantes (Ombudsmen) de otros países para que, desde España, lidere la ética política futura en la materia.

Estamos a disposición de quien pueda necesitar alguna precisión o aclaración sobre lo expuesto y solicitado en esta queja para lo que ofrecemos el teléfono 902998352 email: [apedanica.ong@gmail.com](mailto:apedanica.ong@gmail.com)

## Otras referencias verificables:

### [TÍTULO DE LA TESIS Problemas morales de las intrusiones ...](#)

<http://www.miguelgallardo.es> › [teseo](#)

PDF **TÍTULO DE LA TESIS. Problemas morales de las intrusiones, grabaciones y escuchas. Hacia una Ética del descubrimiento y la revelación de secretos.**

### [UNIVERSIDAD COMPLUTENSE DE MADRID - Miguel A. Gallardo](#)

<http://www.miguelgallardo.es> › tesis

PDF de PM DE LAS INTRUSIONES · 2015 - UNIVERSIDAD COMPLUTENSE DE MADRID. FACULTAD DE FILOSOFÍA. **TESIS DOCTORAL. PROBLEMAS MORALES DE LAS INTRUSIONES, GRABACIONES Y ESCUCHAS. HACIA UNA ÉTICA DEL DESCUBRIMIENTO Y LA REVELACIÓN DE SECRETOS.**

### [fiscal-tribunal-constitucional-google.pdf - CITA](#)

<https://www.cita.es> › [fiscal-tribunal-constitucional-...](#)

PDF 5 sept 2021 — Subject: Sentencias CONSTITUCIONALES CENSURADAS por GOOGLE Fwd: ... página <https://cita.es/escuchas/sentencias> que no es más que una ...

### [Perito en teléfonos móviles IMEI IMSI Teléfono 902998352 ...](#)

<https://www.cita.es> › [perito-moviles](#)

El robo de teléfonos móviles, o el simple acceso eventual a un teléfono celular **SMARTPHONE** para copiar los datos y metadatos que contiene inicia una ..

### [Criptología notarial. Proyectos y riesgos actuales. Prospectiva ...](#)

<https://www.economistjurist.es> › [export](#) › [force](#)

**Criptología notarial.** Proyectos y riesgos actuales. Prospectiva de la fe pública digitalizable. Por Dr. (PhD) Ing. Miguel Ángel Gallardo Ortiz y Achille Campagna, notario en San Marino...

### [La asociación APEDANICA tiene experiencia y conocimientos ...](#)

<https://www.miguelgallardo.es> › [responsabilizador](#)

PDF **RESPONSABILIZACIÓN PERICIAL** para procedimientos administrativos o judiciales penales, sociales, civiles o mercantiles con dictamen "AD HOC".

### [Extorsionabilidad, extorsionistas y extorsionología pericial ...](#)

<http://www.miguelgallardo.es> › [extorsionologo](#)

PDF 23 jul 2018 Estudio inacabado [www.cita.es/extorsiones](http://www.cita.es/extorsiones) **EXTORSIONOSCOPIA FORENSE**

### [Miguel Gallardo PERITO JUDICIAL criptólogo Tel. - 902998352.](#)

<http://www.miguelgallardo.es> › [narcovalijas](#)

PDF 2 ene 2019 — legítimo ejerza derechos **ARCO (Acceso, Rectificación, Cancelación u Oposición)**, por ejemplo, sobre su propio móvil o celular SMARTPHONE y ...

### [Policología y metapolicología - Miguel A. Gallardo \(DEA\)](#)

<http://www.miguelgallardo.es> › [policologia](#)

PDF de MÁG Ortiz · 1998 — Esta idea pretende ser útil para la motivación, interpretación y crítica de un nuevo régimen disciplinario policial, cuyo anteproyecto...

<https://www.miguelgallardo.es/ingeniero-de-minas.pdf>

<https://www.miguelgallardo.es/criminologo.pdf>

<https://www.miguelgallardo.es/cv.pdf>

[@miguelgallardo](#) **Dr. (PhD) Ing. Miguel Gallardo PERITO** Tel. (+34) 902998352 E-mail: [apedanica.ong@gmail.com](mailto:apedanica.ong@gmail.com)

[@APEDANICA](#) **Asociación APEDANICA** con registro del Ministerio del Interior [www.cita.es/apedanica.pdf](http://www.cita.es/apedanica.pdf)