@miguelgallardo Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Presidente de Colombia Gustavo Petro
y su Ministro del Interior Alfonso Prada
solicitud publicada en https://www.miguelgallardo.es/gustavo-petro.pdf

Desde Madrid, con nuestros máximos respetos, deseamos solicitar su atención para los equipos y sistemas para la intervención de las comunicaciones en Colombia, y en especial, para cuanto se haya utilizado el sistema spyware **PEGASUS** de NSO Group, los clonadores de teléfonos SMARTPHONES conocidos como **CELLEBRITE** (**UFED**) y los interceptadores o IMSI Catchers o StingRays como **VERINT**.

APEDANICA (Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas) recomienda al Ministro del Interior requerir un informe detallado sobre todo uso que se hizo de esas tres tecnologías intrusivas en Colombia por responsables de gobiernos anteriores. Podemos ofrecer a las autoridades colombianas todo cuanto hemos documentado de **PEGASUS** **CELLEBRITE** y **VERINT** en varios países, y en especial, en España, donde **hasta el presidente del Gobierno Pedro Sánchez fue espiado, según se investiga en la Audiencia Nacional de España (véase lo publicado sobre las diligencias previas 68/2022)**.

PEGASUS **CELLEBRITE** y **VERINT** no solamente son controvertibles en la jurisdicción nacional de España, sino que suponen un gravísimo problema para el derecho europeo comunitario. En el caso de Colombia los antecedentes documentables podrían llegar a la Organización de las Naciones Unidas ONU, porque esas tres tecnologías son un problema mundial encubierto por muy interesadas “conspiraciones de silencio”.

El Gobierno de Colombia tiene una oportunidad histórica para plantear un debate político y jurídico sobre las intrusiones en la telefonía celular. No hay nada peor que la **IGNORANCIA DELIBERADA** de un problema que se hereda. Podremos estar de acuerdo, o no, con las decisiones que se tomen sobre **PEGASUS** **CELLEBRITE** y **VERINT**, pero lo que siempre definirá bien al gobierno malo, es lo que decida ignorar por su voluntad y su representación. En este sentido, estamos a la disposición de todo colombiano que quiera saber qué se ha espiado ilegalmente, y más aún de las autoridades que afronten problema por las **intrusiones, grabaciones y escuchas** mediante esas 3 controvertidas tecnologías, rogando acuse de recibo para este PDF de 6 páginas, incluyendo ésta.

@miguelgallardo Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf
https://cita.es/cellebrite-fiscal-alejandro-gertz-manero

FISCAL GENERAL DE LA REPÚBLICA DE MÉXICO

Atn. Dr. Alejandro Gertz Manero con copia para IFAI y embajadas de México y España
DENUNCIA publicada en https://www.miguelgallardo.es/cellebrite-mexico.pdf

Como mejor proceda se presenta denuncia por los siguientes HECHOS:

1º APEDANICA ha conocido muy graves incidentes relacionados con los equipos de hardware y sistemas de software CELLEBRITE procedentes de Israel. Adjuntamos la denuncia que hemos enviado a la Fiscalía de la Audiencia Nacional de España según adjunto de **https://www.miguelgallardo.es/fiscal-cellebrite.pdf**
y Fiscalía de Criminalidad Informática **https://cita.es/cellebrite-fiscal-elvira-tejada** con referencias corroborables sobre el hackeo a CELLEBRITE que consideramos **"*notitia criminis*" también para la Fiscalía General de la República de México.**

2º Los Estados Unidos de México han adquirido numerosos equipos y sistemas de CELLEBRITE que han sido objeto de muy diversas controversias aunque, todavía, no tan crispadas como las provocadas por los espionajes realizados con el sistema PEGASUS de NSO Group. Ambas empresas, con sede en Israel, sin ningún control por autoridad alguna, ni de México, ni de Europa, acceden a datos personales muy sensibles, y a diversos secretos muy lícitos y éticos, que merecen protección eficaz.

3º APEDANICA está recopilando información de fuentes abiertas, y bien verificable, que legítimamente indagan en las acciones, omisiones y disfunciones, en especial, por conflictos de intereses, de empresas y organizaciones que acceden a datos que pueden servir para extorsionar incluso a fiscales y jueces. Es fácil comprobar que hemos denunciado y publicado sobre espionaje masivo de Google, NSO Group y CELLEBRITE, y también sobre el llamado "**CONTROL DE TOGAS**" por el que servicios de inteligencia o espionaje condicionan a operadores jurídicos. Podemos inferir que, con gran probabilidad, algún fiscal o juez mexicano haya sido espiado por sistemas como CELLEBRITE o PEGASUS. Sugerimos ver el último ANEXO sobre espionaje a fiscales españoles contra la corrupción y el crimen organizado en la tesis doctoral de 2015 publicada en **https://www.miguelgallardo.es/tesis.pdf**

4º APEDANICA está permanentemente a la disposición de todas las víctimas de tecnopolios que trafican con información sensible que acaba siendo utilizada para extorsionar, también a funcionarios públicos. Sabemos que muchas acusaciones de corrupción tienen más de extorsión que de colusión. Desde hace años investigamos técnicas periciales para **EXTORSIONOSCOPIA** con **INFORMATOSCOPIA**. Véase un resultado ya sentenciado en **http://www.miguelgallardo.es/extorsionado.pdf**

Por lo expuesto, como mejor proceda solicitamos que se tenga por presentada esta denuncia con los documentos adjuntos, y se admita iniciando la Fiscalía General de la República de México la investigación más eficaz sobre los hechos denunciados, informándonos como denunciantes e interesados de cuanto sea publicable sobre CELLEBRITE y PEGASUS de NSO Group, por consideración a este PDF que consta de 5 páginas, incluyendo ésta, rogando su trasladado al funcionario más competente, y su acuse, lo antes posible.

Fiscalía a la que corresponda esta DENUNCIA

Esta denuncia está publicada en https://www.miguelgallardo.es/fiscal-cellebrite.pdf

Como mejor proceda se presenta denuncia por los siguientes HECHOS:

1º Recientemente se han publicado noticias sobre la brecha con fuga de información en la empresa Cellebrite que afecta a muy sensibles datos personales.En 2017 Cellebrite ya fue hackeada, pero ahora, la cantidad de datos comprometidos, unos 4 TB pueden afectar gravemente a millones de datos personales en todo el mundo. Todos esos datos de Cellebrite parecen estar condicionalmente disponibles en
https://ddosecrets.com/wiki/Cellebrite_Mobilogy
https://ddosecrets.com/wiki/Cellebrite_Team_Foundation_Server
aunque puede haber más información hackeada a Cellebrite.

2º Los sistemas de Cellebrite han sido adquiridos y usados desde hace muchos años por Ministerios (ver licitaciones en hiperenlaces) del **Interior** (42) y de **Defensa** (37), Comisión Nacional de los Mercados y la Competencia **CNMC** (44) (véase el relevante documento publicado en **https://cita.es/cellebrite-cnmc-compra.pdf** y otras entidades públicas y privadas diversas. El Gobierno de España ha adquirido sistemas Cellebrite para entregárselos a países como Mauritania y Gambia, según "**21M065-B. Suministro de herramientas y software de uso forense**". Las inversiones y los gastos en Cellebrite son muy considerables y han creado muchas dependencias en varias Administraciones Públicas y autoridades que ahora son más vulnerables. En todo caso, el acceso y la mera custodia de cuanto se haya extraído de cualquier dispositivo mediante sistemas de Cellebrite es una gran responsabilidad creciente.

3º Considerando el amplio uso de Cellebrite en España incluso en inspecciones de la CNMC (véase la solicitud de transparencia adjunta), cuya posición dominante, sin competencia comercial mencionable, y la gravedad de los hechos revelados por muy diversas publicaciones que evidencian las vulnerabilidades que afectan a la seguridad de datos personales, ya hemos presentado otra denuncia ante la Agencia Española de Protección de Datos AEPD, también adjuntada, sin perjuicio de otras actuaciones que nos reservamos. El justificante del registro electrónico de nuestra denuncia puede verse en en **https://cita.es/aepd-cellebrite-justificante.pdf**

4º Los hechos aquí denunciados pueden ser constitutivos de diversos delitos públicos perseguibles de oficio que deben ser investigados por la Fiscalía.

Por lo expuesto, a la Fiscalía que corresponda solicitamos que admita esta denuncia y que abra las diligencias que procedan para requerir a Cellebrite y a las entidades públicas que utilizan sus sistemas, al menos, a los Ministerios (ver licitaciones en hiperenlaces) del **Interior** (42) y **Defensa** (37), Comisión Nacional de los Mercados y la Competencia **CNMC** (44) que documenten la brecha de seguridad y con la mayor precisión posible los datos personales expuestos, directamente o por alguna de las consecuencias o riesgos derivados de los hechos aquí denunciados en este PDF de 4 páginas del solicitamos pronto acuse de recibo, sin perjuicio ni renuncia de otras acciones y derechos, incluso internacionales, que nos reservamos.

Comisión Nacional de los Mercados y la Competencia CNMC

Atn. jefa de área de desarrollo de aplicaciones e inspecciones tecnológicas Laura Estebanez Rogero y subdirector de subdirección de sistemas de las tecnologías de la información y las comunicaciones Andrés Aznar López para esta solicitud publicada en https://www.miguelgallardo.es/cellebrite-cnmc-transparencia.pdf

Como mejor proceda, ejerciendo los derechos de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno **se solicitan los siguientes datos disponibles en la CNMC**:

1º Fecha en la que comenzaron a realizarse inspecciones mediante el sistema Cellebrite (Ufed 4PC, Premium o no, u otros), herramientas de las que la CNMC dispone de varias licencias que solicitamos se precisen por la **fecha de inicio de uso de cada una de ellas**. Nótese que una fecha es la publicada en contrataciondelestado.es y otra la de **primer uso de cada licencia Cellebrite**, que es lo que aquí solicitamos.

2º Número de inspecciones y **total de dispositivos** (móviles o tabletas) clonados, o analizados, desglosando cuanto sea posible, con número de casos en que **el titular del dispositivo autorizó el uso de alguno de los sistemas Cellebrite**, y de los que **denegó su consentimiento**.

3º Número de sanciones que se han basado en algún dato obtenido de algún móvil clonado o analizado por alguno de los sistemas Cellebrite y de ellas, **cuántas se han judicializado** en cualquier jurisdicción, desde los recursos contenciosos administrativos, hasta las penales, desde la primera con su fecha de judicialización, hasta la más reciente conocida.

Aunque la Ley 19/2013 no requiere motivación o justificación alguna, en aras de la eficacia, y para el mejor conocimiento de los responsables de los sistemas Cellebrite en la CNMC, considerando su muy amplio uso y su posición dominante actual, sin competencia comercial mencionable, así como por la **gravedad de los hechos revelados por muy diversas publicaciones que evidencian las vulnerabilidades que afectan a la seguridad de datos personales**, informamos a la CNMC que ya hemos presentado una denuncia ante la Agencia Española de Protección de Datos AEPD que adjuntamos, sin perjuicio de otras actuaciones que nos reservamos. El justificante del registro electrónico de nuestra denuncia puede verse en **https://cita.es/aepd-cellebrite-justificante.pdf**

La asociación APEDANICA, y su presidente personalmente, están a la disposición de todo el que pueda dar o recibir información veraz sobre Cellebrite en relación a lo ya denunciado y aquí **solicitado con pronto acuse de recibo de este PDF de 3 páginas incluyendo ésta**.

@miguelgallardo Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf
https://cita.es/aepd-cellebrite-justificante.pdf https://www.miguelgallardo.es/aepd-cellebrite-personal.pdf

Agencia Española de Protección de Datos AEPD por DENUNCIA

Atn. directora Mar España Martí secretaria general Mónica Bando Munugarren y subdirectora de Inspección de Datos Olga Pérez Sanjuán por denuncia publicada en https://www.miguelgallardo.es/aepd-cellebrite.pdf

Como mejor proceda se presenta denuncia por los siguientes HECHOS:

1º Recientemente se han publicado noticias sobre la brecha con fuga de información en la empresa Cellebrite que afecta a muy sensibles datos personales. **Con fecha 5.8.22** https://www.hackread.com/anonymous-leaks-4tb-cellebrite-data-cyberattack/ ***Cellebrite is an Israel-based smartphone hacking (or cracking) firm that previously made headlines for unlocking iPhone devices for law enforcement and security agencies in the United States. An anonymous source has leaked around 4TB of proprietary data belonging to Israeli digital intelligence firm, Cellebrite. The affected products are the company's flagship product, Cellebrite Mobilogy, and the Cellebrite Team Foundation server.***

https://www.thetechoutlook.com/news/technology/security/an-anonymous-source-leaked-4tb-of-data-from-israeli-intelligence-company-cellebrite/

An anonymous source leaked 4TB of proprietary data from Cellebrite an Israeli digital intelligence company. Cellebrite provides cybersecurity tools for federal, state, and local law enforcement as well as for companies and enterprises. The company provides services to collect, review, analyze, and manage digital data.

2º Los sistemas de Cellebrite han sido adquiridos y usados desde hace muchos años por Ministerios del Interior y de Defensa, Comisión Nacional de los Mercados y la Competencia CNMC y otras entidades públicas y privadas. Puede asegurarse que hay muy numerosos sistemas de Cellebrite que durante años han accedido a muchos TERABYTES de datos personales extremadamente sensibles. Por ejemplo, a cierto perfil de detenidos se les han clonado sus teléfonos móviles. APEDANICA ya denunció tan gravísima inseguridad a la **Defensora del Pueblo, Soledad Becerril Bustamante,** tal y como puede verse en los **enlaces** publicados en **www.cita.es/defensora-del-pueblo** y **www.miguelgallardo.es/defensora-del-pueblo.pdf** y también **a la Agencia Española de Protección de Datos AEPD** según **enlaces** en www.cita.es/aepd-smartphones y www.miguelgallardo.es/aepd-smartphones.pdf www.cita.es/aepd-vodafone y www.miguelgallardo.es/aepd-vodafone.pdf

3º Es muy probable que los **4 TB (cuatro terabytes)** hackeados a Cellebrite afecten a los datos personales y secretos de numerosos españoles (considerando que sus sistemas tienen "mantenimiento remoto" con acceso a datos del sistema en España) y puedan ser **extorsionados por quienes accedan a tan sensible información**. Cellebrite debe informar a los afectados, y todavía no consta ningún comunicado en relación a los gravísimos hechos publicados. Es muy relevante aquí el **precedente comunicado por Vodafone sobre otra brecha de seguridad de Cellebrite** archivado por la Agencia Española de Protección de Datos AEPD en **E-01903-2017**.

Por lo expuesto, solicitamos que se admita esta denuncia y **URGENTEMENTE se requiera a Cellebrite, así como a las entidades públicas y privadas que utilicen sus sistemas en España** y puedan estar afectadas por ser responsables de datos compartidos con Cellebrite, su **informe detallado y publicable sobre los hechos aquí denunciados**, y se nos tenga por personados como interesados legítimos, sin perjuicio de otras acciones y derechos que podamos ejercer, y que nos reservamos.

NOTA: Hemos encontrado, al menos, 144 resultados de licitaciones en que se menciona a Cellebrite en la Plataforma de Contratación del Sector Público así
https://contrataciondelestado.es/wps/portal/!ut/p/b1/pZDLasNADEU_SbLmEc9yPLbHDmnjR8apZ1O8CCElj03p91cxga7iFirQQulcdBFEGJUmSogb3iBep6_Tcfo83a7T-T5H_W6HorW1EYjGZUidIZ0PRGhWDIwM4JOyOPtZn6Y2SyyiCCIa3bbO5Mi-ePhKODmsh0b3tUesqzLfhEShJ_23-wsH7r4sts6VFWHaC15v8hB0xaNXD_8pQP_01W_59xBnZOkDM7D04uWQBK_V7XKAkbHVT5Zt1jG2bI52jacEUclOxglu8VxymfpDTt-ImUUq/dl4/d5/L2dBISEvZ0FBIS9nQSEh/pw/Z7_BS88AB1A0OUMA0IL1IQEP210C1/act/id=0/520986484533/-/?ACTION_NAME=ScopeSearchAction&SearchFieldPrefix=ns_Z7_BS88AB1A0OUMA0IL1IQEP210C1_&ns_Z7_BS88AB1A0OUMA0IL1IQEP210C1_pageNumber=1&ns_Z7_BS88AB1A0OUMA0IL1IQEP210C1_scopeId=&ns_Z7_BS88AB1A0OUMA0IL1IQEP210C1_ExecuteQuery=1&ns_Z7_BS88AB1A0OUMA0IL1IQEP210C1_query=CELLEBRITE&ns_Z7_BS88AB1A0OUMA0IL1IQEP210C1__submitSearch=Buscar

REFERENCIAS SOBRE CELLEBRITE: Ofrecemos al menos 21 documentos como resultados nuestros (de APEDANICA) en el metaenlace "autoactualizable"
https://www.google.com/search?q=CELLEBRITE+site%3Acita.es+%7C+site%3Amiguelgallardo.es
entre los que aquí destacamos

https://www.cita.es/aepd-smartphones

AEPD y registro policial de teléfonos móviles smartphones de ...

Es decir, que Europol conoce los sistemas de **Cellebrite**, autónomos o en PC, que tiene como único propósito acceder a los datos de cualquier móvil …

https://www.cita.es/defensora-del-pueblo

Defensora del Pueblo Soledad Becerril y perito por detenidos ...

Es conocida la marca del fabricante "**Cellebrite**" que se jacta de suministrar a policías diversos sistemas para la extracción de datos de smartphones, …

http://www.miguelgallardo.es/apedanica-smartphone.pdf

HABEAS SMARTPHONE de la asociación APEDANICA con Tel.

28 mar 2017 — UNIDAD ORGÁNICA DE POLICÍA JUDICIAL ("**Cellebrite** UFED Reports") del examinador M41779L con fecha 01/02/2017 y diversas manifestaciones ..

PUBLICACIONES CITABLES SOBRE CELLEBRITE

… ***Cellebrite*** *UFED is recognized as the most advanced commercial mobile forensics tool* … SAHARAN, Sameer; YADAV, Bhuvnesh. Digital and Cyber Forensics: A Contemporary Evolution in Forensic Sciences. En *Crime Scene Management within Forensic Science*. Springer, Singapore, 2022. p. 267-294.

… Documents show they purchased ***Cellebrite****'s phone-****hacking*** *tech and received training Israeli phone-****hacking*** *firm* ***Cellebrite*** *sold its technology to Bangladesh's notorious paramilitary…* HASHMI, Taj. "Dynastic Democracy" Under the "Battling Begums," 1991–2021. En *Fifty Years of Bangladesh, 1971-2021*. Palgrave Macmillan, Cham, 2022. p. 191-242.

… **This article also appears to suggest that Cellebrite may have been using software written by hackers to remove software restrictions on Apple devices**…
BROWN, Steven David. Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice. En *ERA Forum*. Springer Berlin Heidelberg, 2020. p. 423-438.

… a contract with ***Cellebrite****, and Centrelink apparently uses spyware to* ***hack*** *the phones of …* MANN, Monique; MOLNAR, Adam; WARREN, Ian. Spyware merchants: the risks of outsourcing government hacking. *The conversation*, 2017, p. 1-1.

In 2017, the Cyber security company Cellebrite was hacked and data was published…
SAALBACH, Klaus-Peter. Attribution of cyber attacks. En *Information Technology for Peace and Security*. Springer Vieweg, Wiesbaden, 2019. p. 279-303.

Esta última publicación y la resolución **E-01903-2017** evidencian ciertos antecedentes de los hechos aquí denunciados. Cellebrite debe ser investigada como solicitamos a la Agencia Española de Protección de Datos AEPD en este documento de 2 páginas con nuestra **denuncia publicada en https://www.miguelgallardo.es/aepd-cellebrite.pdf**

@miguelgallardo Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf