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

Remitente:
APEDANICA ONG APEDANICA ONG

Destinatarios:

Con copia a:

Fecha de Recibido:
24/08/2022 08:46:47 AM

Correo Peticionario: Contacto(contacto@presidencia.gov.co)
De (Remitente): APEDANICA ONG APEDANICA ONG (apedanica.ong@gmail.com)
Enviado el: 24/08/2022 8:46:47 a.m.
Para: contactonueve@presidencia.gov.co
Asunto: RV: Presidente de Colombia Gustavo Petro y su Ministro del Interior Alfonso Prada solicitud publicada en https://www.miguelgallardo.es/gustavo-petro.pdf

De: apedanica ong

Enviado el: martes, 23 de agosto de 2022 9:10 p. m.
Para: Contacto

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

1 ANEXO en PDF de 6 páginas
https://www.miguelgallardo.es/gustavo-petro.pdf
SOLICITANDO PRONTO ACUSE DEL ANEXO

@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.

https://cita.es/cellebrite-fiscal-alejandro-gertz-manero

De: apedanica ong >
Date: lun, 8 ago 2022 a las 14:24
Subject: DENUNCIA por CELLEBRITE en México para FISCAL GENERAL DE LA REPÚBLICA Atn. Dr. Alejandro Gertz Manero por María Fernanda Pérez Galindo https://www.miguelgallardo.es/cellebrite-mexico.pdf
To: >, >, >, >, >, >, >, >
Cc: MIGUEL ANGEL GALLARDO ORTIZ >, Fiscalía ante la Audiencia Nacional >, >, >, >

ANEXO DENUNCIA en PDF de 5 páginas
https://www.miguelgallardo.es/cellebrite-mexico.pdf
Atn. Dr. Alejandro Gertz Manero por María Fernanda Pérez Galindo Encargada de la Dirección General de Cooperación Internacional de la FISCAL GENERAL DE LA REPÚBLICA DE MÉXICO, embajadas e IFAI rogando su pronto acuse de recibo

@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

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 traslado al funcionario más competente, y su acuse, lo antes posible.

El lun, 8 ago 2022 a las 10:01, apedanica ong (>) escribió:
DENUNCIA con 2 ANEXOS para Jesús Alonso Cristóbal Fiscal de Sala Jefe de la Fiscalía Ante la Audiencia Nacional SOLICITANDO PRONTO ACUSE DE RECIBO DE LOS 2 ANEXOS sobre CELLEBRITE (reiterando más abajo lo ya denunciado sobre PEGASUS de NSO Group)
· https://www.miguelgallardo.es/fiscal-cellebrite.pdf
· https://cita.es/cellebrite-cnmc-compra.pdf
· REITERANDO LO YA ENVIADO el mié, 13 jul 2022 a las 13:17
· https://www.miguelgallardo.es/pegasus-policial.pdf
https://cita.es/pegasus-policial-noticia.pdf
https://cita.es/pegasus-policial-aepd.pdf
· INSISTIENDO EN SOLICITAR ACUSE DE RECIBO DE LOS 2 CORREOS
·

@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

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.

@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-cnmc-compra.pdf

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

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_SbLmEc9yPLbHDmnjR8apZ1O8CCElj03p91cxga7iFirQQuIcdBFEGJUmSogb3iBep6_Tcfo83a7T-T5H_W6HorW1EYjGZUidlZ0PRGhWDIwM4JOyOPtZn6Y2SyyiCCla3bbO5Mi-ePhKODmsh0b3tUesqzLfhEShJ_23-wsH7r4sts6VFWHaC15v8hB0xaNXD_8pQP_01W_59xBnZOkDM7D04uWQBK_V7XKAkbHVT5Zt1jG2bl52jacEUcIOxgIu8VxymfpDTt-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

El mié, 13 jul 2022 a las 13:17, apedanica ong (>) escribió:
3 ANEXOS para Jesús Alonso Cristóbal Fiscal de Sala Jefe de la Fiscalía Ante la Audiencia Nacional SOLICITANDO PRONTO ACUSE DE RECIBO DE LOS 3 ANEXOS

Si nuestra información es correcta, Jesús Alonso Cristóbal es el fiscal personado que actúa y propone diligencias o preguntas a testigos en las DILIGENCIAS PREVIAS PROC. ABREVIADO 68/2022 del JUZGADO CENTRAL DE INSTRUCCIÓN Nº 4 AUDIENCIA NACIONAL (espionaje por PEGASUS) y queremos que conozca y reconozca los 3 anexos que desde el pasado lunes ya tiene FGE Unidad de Criminalidad Informática > haciéndole saber nuestra preocupación por la absoluta falta de coordinación entre varios fiscales que ya conocen hechos todavía no instruidos, como es el caso Alfonso San Román, mencionado en los muy relevantes ANEXOS ya enviados a fge.ucrinf@fiscal.es así:

De: apedanica ong >
Date: lun, 11 jul 2022 a las 10:57
Subject: PEGASUS POLICIAL para ESPIONAJES DELICTIVOS en 3 ANEXOS para FISCALElvira Tejada Re: Ampliando sobre PEGASUS y NSO Group con ANEXO PDF Re: Elvira Tejada Fiscal de Criminalidad Informática y FACEBOOK denuncia en www.cita.es/facebook-filtraciones.pdf

To: FGE Unidad de Criminalidad Informática >
Cc: >, >, >, >, >, >, >, >

3 ANEXOS en PDF
https://www.miguelgallardo.es/pegasus-policial.pdf
https://cita.es/pegasus-policial-noticia.pdf
https://cita.es/pegasus-policial-aepd.pdf
SOLICITANDO PRONTO ACUSE DE RECIBO DE LOS 3 ANEXOS a
Fiscalía para la Criminalidad Informática Atn. Fiscal-Jefe Elvira Tejada

@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

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

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 espiados. 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.

ANEXO https://cita.es/pegasus-policial-noticia.pdf

10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 1/18 -31% -28% -39% -33% INVESTIGACIÓN Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy Empresarios israelíes y la cúpula policial pactaron que la entrega del material que permitía irrumpir en los teléfonos móviles debía realizarse en un hotel de Barcelona, según la documentación incluida en una denuncia que presentó el exjefe de Asuntos Internos Marcelino Martín-Blas 6 Se lee en minutos El exnúmero dos de la Policía Eugenio Pino, a su salida de la declaración en la Audiencia Nacional. / DAVID CASTRO Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 2/18 -31% -28% -39% -33% Un artículo de Tono Calleja Flórez J. G. Albalat Madrid / Barcelona 26 de abril del 2022 a las 06:50. Actualizada a las 16:48 ? ? ? ? ? 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. ? Comentarios ? PUBLICIDAD Ad 0 Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 3/18 -31% -28% -39% -33% EL PERIÓDICO DE ESPAÑA ha tenido acceso a una carta de invitación enviada el 31 de julio de 2014 por Caspy, uno de los propietarios de la firma Rayzone Group, dirigida al entonces director adjunto operativo (DAO) de la Policía, Eugenio Pino, en la que la firma israelí fijaba una cita para el 11 de agosto del mismo año con la intención de realizar "una prueba de campo" que incluía "una demostración en vivo de un sistema GSM pasivo táctico", especifica la misiva. Otro documento apunta que la entrega del material, que debía ser introducido por el Aeropuerto de Barajas, iba a realizarse en un hotel de Barcelona. El escrito del directivo de Rayzone también pone de manifiesto que la firma israelí realizaba este ofrecimiento tras los "encuentros" y "demostraciones" que habían mantenido en fechas anteriores con la cúpula policial liderada por Eugenio Pino, que está procesado en la Audiencia Nacional por ser presuntamente uno de los responsables del espionaje que realizaron las cloacas policiales en 2013 al extesorero del PP Luis Bárcenas, que en esas fechas amenazaba con implicar en el caso Gürtel a los dirigentes del partido entonces liderado por Mariano Rajoy. La newsletter de Política Gemma Robles analiza qué certezas, medias verdades o bulos tratan de hacernos llegar los que están a los mandos en su newsletter de política. SUSCRÍBETE Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 4/18 -31% -28% -39% -33% Matian Caspy habría ejercido de intermediario desde 2010 para la venta del sistema Pegasus al Gobierno de un país, según relata una información publicada en Israel, que apunta también que este informático y su empresa Rayzone logró cobrar un 60% de la comisión por una venta del sistema de espionaje, en la que también habría participado un empresario al que se vincula con el expresidente de Estados Unidos Donald Trump. PUBLICIDAD Ad Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 5/18 -31% -28% -39% -33% ASUNTOS INTERNOS En España, la venta presuntamente fraudulenta a la cúpula policial del Gobierno de Rajoy se dio a conocer gracias a la denuncia que presentó el 31 de octubre de 2017 el que fuera jefe de Asuntos Internos del Cuerpo Nacional de Policía (CNP) Marcelino Martín-Blas en el Juzgado de Instrucción número 2 de Madrid, en el seno de la investigación que se realizó al constatar que agentes del Centro Nacional de Inteligencia (CNI) habían sido grabados sin orden judicial. Y en su denuncia el comisario principal aportaba documentos que apuntaban a la compra subrepticia de esta tecnología de espionaje. Este comisario principal aseguró en su denuncia que tanto Eugenio Pino como su jefe de gabinete, José Ángel Fuentes Gago, disponían desde 2014 de la tecnología suficiente para poder interceptar y grabar conversaciones e información de teléfonos inteligentes y otros dispositivos electrónicos "sin autorización judicial como consecuencia de habérsela adquirido a la empresa israelí Rayzone Group", relata el escrito firmado por el abogado Antonio Alberca. Política ? Política Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 6/18 -31% -28% -39% -33% Este letrado aportó la documentación que un funcionario policial había recibido desde las cuentas profesionales de Pino y su 'número dos' que previamente había sido remitida por la empresa israelí que se encargaba del presunto espionaje. Y según el letrado del abogado de Martín-Blas, durante los meses de julio, agosto y septiembre de 2014 el inspector Fuentes Gago, "a los efectos de no dejar rastro de las conversaciones entre la cúpula policial- y la empresa Rayzone Group LTD, que se mantenían para adquirir tecnología destinada a interceptar teléfonos móviles y otros dispositivos electrónicos", le pidió a un funcionario que descargara en un USB una documentación que se adjuntaba como borrador en un correo electrónico privado de Google. De esta forma, evitaban que la documentación pudiera ser interceptada en internet. EN UN HOTEL DE BARCELONA Entre la información que el funcionario aseguró haber recibido se incluía la carta remitida por Matian Caspy a Eugenio Pino, pero también un escrito dirigido a la empresa Rayzone en el que se pone de manifiesto que la cúpula policial estaba al tanto de la compra fraudulenta del material: "Como continuación a la conversación mantenida en el día de ayer, nuestros jefes nos piden que os informemos de lo siguiente: quieren mantener una reunión el día 3 de septiembre para ver resultados y poder informar, igualmente ellos de los resultados a sus superiores". PUBLICIDAD Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 7/18 -31% -28% -39% -33% Después, el escrito alude a los supuestos abonos que las cloacas policiales iba a realizar para obtener el material para el espionaje: "El pago del día 6 se hará como acordemos por este medio, en la cantidad de 90. El pago del día 15 será de 15 y no de 35. Los 20 restantes se entregarán el día 3 en la reunión que mantengamos". Y, finalmente, el documento aportado al juzgado madrileño informaba de cómo se tenía que llevar a cabo la operación: "Nos dicen que para pasar el material de forma segura, se ha de utilizar el Aeropuerto de Madrid y después llevar el material a Barcelona. El hotel en Barcelona, sin problemas. Solamente nos tenéis que decir cuántas personas vienen y cuántos días, así como las fechas". Este escrito, según el exjefe de Asuntos Internos, daba a entender que la compra de la tecnología a la empresa israelí había sido finalmente aprobada y que iba a ser introducida de forma "subrepticia" en España. Ad Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 8/18 -31% -28% -39% -33% Precisamente, la Fiscalía Anticorrupción ha pedido una pena de 10 años de cárcel en una pieza separada del caso Villarejo para el exjefe del aeródromo madrileño Carlos Salamanca por permitir la entrada de forma irregular de ciudadanos de Guinea Ecuatorial a cambio de regalos de alto valor económico. ANOTACIONES DE VILLAREJO La publicación el 31 de octubre de 2017 en el diario El País de la denuncia interpuesta por Marcelino Martín-Blas en el Juzgado de Madrid contra Eugenio Pino por contratar a la empresa de espionaje israelí tuvo su reflejo en la agenda de Villarejo, que según explican fuentes del caso a EL PERIÓDICO DE ESPAÑA usaba como guía de sus grabaciones. En concreto, el comisario jubilado escribió: "Pino: llamó por noticia de El País dónde dice [el periodista] Ayuso que Marcel [Marcelino MartínBlas] aportó la factura de la compra de un equipo de control de teléfonos". Un poco más abajo, en relación con el entonces número dos del Ministerio del Interior, Francisco Martínez, a quien identifica con el apodo de "Chisco", redacta: "Sobre datos de la compra de equipos. No ha contestado a mi mensaje". En octubre de 2017, Francisco Martínez ya llevaba un año fuera del Ministerio del Interior. Sin embargo, la petición del exjefe de Asuntos Internos no convenció al fiscal Alfonso San Román, -que investigaba la grabación irregular al CNI-, a imputar a Eugenio Pino y a su 'número dos'. Y no les llamó a declarar, pese a que un informe del Centro Criptológico Nacional, un organismo dependiente del propio CNI, consideraba posible técnicamente que uno de los teléfonos policiales que habría sido atacado tuviera instalada "una aplicación dañina y que esa aplicación u otra haya borrado todo vestigio de la misma. Es una posibilidad técnica que desconocemos si fue o no utilizada porque, como ya se ha dicho, no hay rastro alguno". Portada Para ti Regístrate ? PUBLICIDAD 10/7/22, 10:07 Un intermediario de Pegasus facilitó un sistema de espionaje a las 'cloacas' policiales de Rajoy | El Periódico de España https://www.epe.es/es/politica/20220426/intermediario-pegasus-espionaje-cloaca-policial-rajoy-13565728 9/18 -31% -28% -39% -33% El fiscal llegó a defender la compra del material para espiar, dando por hecho que habría sido utilizado bajo supervisión judicial: "El hecho de que el Cuerpo Nacional de Policía compre un concreto software, si finalmente esto pudiera acreditarse después de la práctica de las diligencias que se solicitan, no es, en sí mismo, ningún delito. La utilización de ese software por la Policía para el cumplimiento de sus funciones y conforme a los requisitos legales, tampoco lo sería", concluía. Noticias relacionadas Temas Pegasus José Manuel Villarejo Policía Ministerio del Interior ? Félix Bolaños: "Somos partidarios de reformar la sedición, pero no hay mayoría hoy para abordarla" Los charcos políticos en los que Yolanda Díaz se tendrá que mojar: referéndum catalán, monarquía o elección de los jueces ? Te recomendamos Recomendado por Oferta Hotel Hasta 40% ¡Reserva ahora! Patrocinado por Barceló Hotel Group Configura tu nuevo Hyundai KONA Configúralo ya Patrocinado por Hyundai ES VER COMENTARIOS ? 0 Comentarios Portada Para ti Regístrate ? PUBLICIDAD

3 ANEXOS en PDF
https://www.miguelgallardo.es/pegasus-policial.pdf
https://cita.es/pegasus-policial-noticia.pdf
https://cita.es/pegasus-policial-aepd.pdf
SOLICITANDO PRONTO ACUSE DE RECIBO DE LOS 3 ANEXOS

El jue, 28 abr 2022 a las 10:36, FGE Unidad de Criminalidad Informática (>) escribió:
Recibido, gracias

De: apedanica ong >
Enviado el: miércoles, 27 de abril de 2022 12:52

Para: FGE Unidad de Criminalidad Informática >
CC: mailsigned@egarante.com

Asunto: Ampliando sobre PEGASUS y NSO Group con ANEXO PDF Re: Elvira Tejada Fiscal de Criminalidad Informática y FACEBOOK denuncia en www.cita.es/facebook-filtraciones.pdf

1 ANEXO en PDF sobre PEGASUS y NSO Group para Elvira Tejada Fiscal de Criminalidad Informática
https://cita.es/defensor-pegasus.pdf
SOLICITANDO PRONTO ACUSE DEL ANEXO

Como ampliación de nuestro mensaje de jueves, 8 de abril de 2021 13:55 del que recibimos acuse el 9 abr 2021 a las 9:24 según puede verse más abajo en el cuerpo de este mensaje, como mejor proceda adjunto documento sobre el espionaje presuntamente realizado con software spyware PEGASUS y NSO Group que ya ha sido registrado en el Defensor del Pueblo a la atención del Prof. Dr. Ángel Gabilondo, así como para Ministra de Defensa Margarita Robles, Ministro de Presidencia Félix Bolaños, Directora de la Agencia Española de Protección de Datos AEPD Mar España Martí solicitando también pronto acuse de recibo del ANEXO con lo siguiente, que incluye su acuse de 9 abr 2021 a las 9:24.

@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

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

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, 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

No es admisible que la AEPD eluda su alta responsabilidad ante los hechos denunciados entonces archivando la denuncia de APEDANICA 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 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

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

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

PEGASUS and NSO Group cellular spying

Document published at www.cita.es/pegasus.pdf

Palestinian BDS National Committee BNC

Document published at 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

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 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 .

Policiología y metapoliciología - Miguel A. Gallardo (DEA)

http://www.miguelgallardo.es > policiologia

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

@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

El vie, 9 abr 2021 a las 9:24, FGE Unidad de Criminalidad Informática (>) escribió:
Acusamos recibo

De: apedanica ong >
Enviado el: jueves, 8 de abril de 2021 13:55
Para: FGE Unidad de Criminalidad Informática >
CC: mailsigned@egarante.com

Asunto: Elvira Tejada Fiscal de Criminalidad Informática y FACEBOOK denuncia en www.cita.es/facebook-filtraciones.pdf

Elvira Tejada Fiscal de Criminalidad Informática y FACEBOOK
denuncia (art. 197 de Código Penal) en ANEXO de 34 páginas en
http://www.cita.es/facebook-filtraciones.pdf
ya registrado en la Agencia Española de Protección de Datos AEPD
http://www.miguelgallardo.es/facebook-filtraciones-justificante.pdf
SOLICITANDO PRONTO ACUSE DE RECIBO

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Agencia Española de Protección de Datos AEPD

y Fiscalía para la Criminalidad Informática DENUNCIA publicada en www.cita.es/facebook-filtraciones.pdf

La Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA, como mejor proceda DENUNCIA estos HECHOS:

1º businessinsider.com ha publicado lo que puede verse en

https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

posteriormente se ha conocido que 11 millones de españoles han sido afectados siendo especialmente relevante lo publicado en

https://rebelionenlagranja.com/noticias/escandalo-facebook-filtran-datos-de-533-millones-de-usuarios-11-millones-espanoles-20210403

Escándalo Facebook: filtran datos de 533 millones de usuarios, 11 millones españoles

En contacto con expertos internacionales hemos podido conocer un sistema para verificar si un número de móvil se ha visto afectado en América, pero los usuarios españoles no pueden consultar en el sistema https://leaks.titan.co/fb/ y en todo caso, merecen explicaciones tanto de Facebook como de las autoridades que no se han pronunciado.

Los perjuicios y los riesgos pueden ser muy grandes. Véase el enlace

https://www.eldiario.es/tecnologia/ciberdelincuente-base-datos-robada-facebook-sea-vieja_1_7376864.html

Todo lo que un ciberdelincuente puede hacer con datos robados de Facebook: "Da miedo el nivel al que permite segmentar" La filtración masiva de información personal de 533 millones de usuarios de Facebook permitirá realizar ataques de ingeniería social mucho más dirigidos, avisan los expertos

2º APEDANICA ha denunciado, desde 2011, hechos muy graves en Facebook y WhatsApp y la AEPD siempre nos ha dirigido a la autoridad irlandesa sin que nunca recibiéramos respuesta alguna. La última está publicada en http://www.miguelgallardo.es/helen-dixon/

Sin embargo, no se ha recibido respuesta alguna de la autoridad irlandesa en un asunto tan grave y trascendental en España.

3º No es admisible que la AEPD eluda su alta responsabilidad ante los hechos de los que Faceboook es responsable archivando las denuncias de APEDANICA en el expediente E/06068/2019 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

Por lo expuesto, SOLICITAMOS que teniendo por presentada esta denuncia con la documentación adjunta en PDF de 34 páginas, se inicie un procedimiento sancionador contra Facebook y contra quien resulte más responsable de los hechos denunciados, en el que se nos tenga por personados como denunciantes perjudicados, y que las autoridades de protección de datos y fiscalías, si hubiera algún indicio racional de delitos, en especial, del 197 del Código Penal, se coordinen eficazmente para que los usuarios españoles de productos y servicios de Facebook reciban pronto información precisa, con todos los detalles y referencias verificables sobre los hechos aquí denunciados, así como sobre los del expediente con Ref.: E/06068/2019 requiriendo todos los informes disponibles a cuantas autoridades españolas, o de otros países, sea procedente, a la mayor brevedad posible, todo ello sin perjuicio ni renuncia a cualquier otro derecho o acción que podamos ejercer.

Solicitamos también que este escrito y toda la documentación adjunta se traslade eficazmente y a la mayor brevedad por la AEPD a

Helen Dixon, Data Protection Commissioner in Ireland

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

y que le requiera pronta respuesta a lo enviado y publicado en inglés

http://www.miguelgallardo.es/helen-dixon/

informándonos de qué correo electrónico mejor que

info@dataprotection.ie

puede servir en el futuro para comunicarnos considerando la relevancia y trascendencia de lo que aquí se denuncia y lo que se adjunta.

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.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

Spanish non-for-profit organization Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA, claimed on 19.5.2019 to Agencia Española de Protección de Datos AEPD about Pegasus spyware of NSO Group as you can see at www.cita.es/whatsapp-espionaje.pdf

AEPD replied (more than 1 year after our claim) that the only European Data Protection Authority investigating Pegasus of NSO Group is the Irish one and forwarded the documents of APEDANICA as was said in a letter signed by Mar España Martí ("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") that we publish at www.cita.es/whatsapp-aepd-irlanda.pdf

De Omni Re Scibili ("of all things that can be known") from APEDANICA we ask you here for the identification of any procedure opened at Data Protection Commission about NSO Group products and the name of the Irish official that can inform about as much as possible. We shall be pleased to share our most relevant documents regarding WHATSAPP INC. and FACEBOOK, INC., both Delaware corporations in the Plaintiff, vs. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, beyond what has already been published at

https://context-cdn.washingtonpost.com/notes/prod/default/documents/bf5edf35-5672-49fa-aca1-edefadff683f/note/8ef25c0d-fee9-416a-b7f9-e0a4dedc66f2.pdf

As far as we know, there are more than 1.400 smartphones spied by NSO and its customers all over the World, but our concern is beyond the owners of those devices. APEDANICA represents anybody who has been in touch with them or was mentioned in private spied conversations because third parties are also affected as victims of conversations they are not part in. If the smartphone of the Data Protection Commissioner is spied, anyone speaking, or in a chat, with him is also a victim, but any third parties mentioned (like APEDANICA members) are also victims, so we want access to any file or record about and, if possible, cooperating as much as you let us. We attach 31 relevant pages for it, waiting for news at phone +34902998352 and email apedanica.ong@gmail.com

www.vice.com/amp/en_us/article/pkyzxz/spain-nso-group-pegasus-catalonia

Source: Spain is Customer of NSO Group The Guardian and El Pais reported NSO Group's malware was used to target prominent politicians in Spain. Now a former employee says that Spain has been an NSO Group customer. By Lorenzo Franceschi-Bicchierai and Joseph Cox Jul 14 2020, 7:01pm The cellphones of several politicians in Spain, including that of the president of one of the countries' autonomous regional parliaments, were targeted with spyware made by NSO Group, an Israeli company that sells surveillance and hacking tools to governments around the world, according to The Guardian and El Pais . Motherboard confirmed the specifics with security researchers who investigated the attempted hack and a Facebook employee who has knowledge of the case. A former NSO employee has told Motherboard that the Spanish government has been an NSO customer since 2015. "We were actually very proud of them as a customer," the former employee said. "Finally a European state." Motherboard granted the source anonymity to protect them from retaliation from the company. We cannot confirm whether these specific attempted hacks were directed by the Spanish government, though one of the politicians targeted believes the Spanish government is behind the attack. Do you work at NSO Group, did you used to, or do you know anything else about the company? On Monday, the media outlets revealed that someone tried to hack the cellphone of Roger Torrent, the President of the Parliament of Catalonia, using a flaw in WhatsApp, which was discovered last year. Torrent is the president of the Parliament of Catalonia, which governs Barcelona and the surrounding region that has recently attempted to become independent from Spain. Carles Puigdemont, a member of the European Parliament and the former president of Catalonia, condemned the hacking attempt, and implied that the Spanish government targeted Torrenthim. If that's the case, this would be the first known case of a European government using this type of technology against politicians inside Europe. "Spain has been using authoritarian methods for a while. I myself had a tracking device on my car which is being investigated by the Belgian authorities," Puigdemont told Motherboard in an email. "The EU cannot wait anymore to act, we have new proofs every day that the rule of law in Spain is totally wrecked." "It is not the first time that accusations of spying on political opponents emerge in Spain. In 2009 there was a spying scandal within the center-right Popular Party. In 2012, Catalan lawmakers have accused the Spanish government of espionage," Mathias Vermeulen, a former aide for a member of the European Parliament who focused on surveillance tech issues, told Motherboard. "But using extraordinary tools like Pegasus against democratically elected politicians is a first in Europe and should be immediately investigated." "Finally aEuropean state." Citizen Lab, a research group that has investigated government spyware for a decade, said it could not definitively confirm who actually deployed the NSO spyware. "Although we can positively verify that Mr. Torrent's phone was targeted by NSO's spyware, we are unable to determine by whom," said Ronald Deibert, the director of the Citizen Lab. A Facebook employee confirmed to Motherboard that Torrent was targeted with NSO spyware on WhatsApp. The employee spoke on condition of anonymity because they were not authorized to talk to the press. ADVERTISEMENT "This is a case where we would infer the customer is Spain but I don't have hard evidence," said a security researcher who has investigated previous cases of hacks done with NSO spyware. The researcher asked to remain anonymous because he wasn't allowed to speak to the press. 9/9/2020 Source: Spain is Customer of NSO Group. NSO Employee AbusedPhone HackingTech toTarget a Love Interest BY JOSEPH COX The former NSO employee said Spain had access to a 0-click version of NSO's Pegasus product. Pegasus is the suite of tools that lets customers remotely break into and surveill phones. Beyond domestic use, the former employee added that the Spanish customer had a number of different territories unlocked for deploying Pegasus in, including France, Malta, and Mexico. NSO prices its Pegasus product based on how many countries or areas the client is able to hack phones in. The client also bought products from Circles, another surveillance company related to NSO, the former employee said. Circles focuses on products that exploit the SS7 network and protocol, and which can be used to track the location of phones. The former employee added that the sale related to a central intelligence agency of Spain. The CNI, or National Intelligence Centre, is Spain's intelligence agency. Two NSO executives and a company spokesperson declined to comment on whether the Spanish government was one of their customers. In a statement sent to reporters, NSO said that "Due to the confidentiality constraints, we cannot confirm or deny which such authorities use our Technology." "We were actually very

proud of them as a customer." "We are appreciative that this matter has been brought to our attention. In line with our Human Rights Policy we take our responsibilities seriously and if warranted, will initiate an investigation," the statement read. "We will cooperate with any competent authority investigation if initiated, in parallel to our internal procedures." The CNI used to be a customer of Hacking Team, the infamous Italian spyware company that dominated the market in the 2000s. In fact, according to former employees of Hacking Team as well as leaked documents published after the company was hacked in 2015, the CNI became Hacking Team's first customer outside of Italy after the terrorist attack in Madrid on March 11, 2004. The CNI and the Spanish government did not respond to a request for comment. The Spanish prime minister's office told the Guardian that "the government has no evidence that the speaker of the Catalan parliament, Roger Torrent, the former MP Anna Gabriel and the activist Jordi Domingo have been the targets of hacking via their mobiles." "Furthermore, we must state that any operation involving a mobile phone is always conducted in accordance with the relevant judicial authorisation." Update: This piece has been updated to include more information from the former NSO Group employee. Subscribe to our cybersecurity podcast, CYBER. TAGGED: EUROPE, SPAIN, HACKING, HACKERS, CATALONIA, PEGASUS, NSO, WORLDNEWS, WORLD PRIVACY 9/9/2020

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.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

La Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA, está investigando todo cuanto pueda conocerse y sea relevante para el enjuiciamiento del espionaje de teléfonos móviles. Se adjunta lo ya enviado a Facebook-Whatsapp sobre PEGASUS-NSO en el correo que puede verse en www.cita.es/whatsapp-pegasus

APEDANICA recopila y se opone a las resoluciones administrativas y judiciales que afecten a la seguridad jurídica y pide interdicción de la arbitrariedad en favor de todo tipo de perjudicados, no solamente en el caso de que sus propios teléfonos hayan sido ilegalmente intervenidos, sino también porque alguna vez se hayan comunicado con un espiado que quiera ejercer derechos como víctima de espionaje secundario. Es decir, que nos preocupa quien haya mantenido algún contacto con un teléfono en el que se haya instalado un software como PEGASUS o FLEXISPY Mobile Spy Spy Phone o se clonase con CELLEBRITE o en cualquier otra intrusión inadmisible e indemnizable. APEDANICA y yo estamos a la disposición de los afectados, tanto en el caso de los 1.400 espiados, directamente o no, por NSO o sus clientes, como en los de los productos con funcionalidad similar, y también nos ofrecemos como peritos en estas tecnologías para todos los que alguna vez hayan establecido algún tipo de comunicación con cualquiera de los espiados.

APEDANICA, con máximo respeto hacia todos sus derechos y libertad, le pide una muy especial consideración no solamente hacia la dignidad de su cargo y a la de todos y cada uno de los ciudadanos que le votaron, sino también para todos aquellos que alguna vez, o muchas veces, se comunicaron con usted por el teléfono que presuntamente fue intervenido ilegalmente, y agradeceremos todo cuanto pueda ser compartido con nosotros, al menos, en lo más doctrinal. Mi tesis, en

www.miguelgallardo.es/tesis.pdf

con todo cuanto pudiera estar a mi alcance desde que la defendí en 2015, incluyendo varios dictámenes periciales, en lo que no perjudique a terceros, y cuanto se adjunta, está a su entera disposición, rogando su más pronto acuse de recibo para estas 19 páginas en PDF.

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.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

From Madrid, Spain, Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA, is seriously interested in any issue regarding WHATSAPP INC. and FACEBOOK, INC., both Delaware corporations in the Plaintiff, vs. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, beyond the document that has already been published at

https://context-cdn.washingtonpost.com/notes/prod/default/documents/bf5edf35-5672-49fa-aca1-edefadff683f/note/8ef25c0d-fee9-416a-b7f9-e0a4dedc66f2.pdf

Between in and around April 2019 and May 2019, Defendants used WhatsApp servers, located in the United States and elsewhere, to send malware to approximately 1,400 mobile phones and devices ("Target Devices"). Defendants' malware was designed to infect the Target Devices for the purpose of conducting surveillance of specific WhatsApp users ("Target Users"). Unable to break WhatsApp's end-to-end encryption, Defendants developed their malware in order to access messages and other communications after they were decrypted on Target Devices. Defendants' actions were not authorized by Plaintiffs and were in violation of WhatsApp's Terms of Service. In May 2019, Plaintiffs detected and stopped Defendants' unauthorized access and abuse of the WhatsApp Service and computers.

.

Plaintiffs request judgment against Defendants as follows: 1. That the Court enter judgment against Defendants that Defendants have: a. Violated the Computer Fraud and Abuse Act, in violation of 18 U.S.C. § 1030; b. Violated the California Comprehensive Computer Data Access and Fraud Act, in violation California Penal Code § 502; c. Breached their contracts with WhatsApp in violation of California law; d. Wrongfully trespassed on Plaintiffs' property in violation of California law.

APEDANICA is considering some European and Latin America legal complaints and/or plaintiffs against PEGASUS spyware so we shall appreciate any updated information about that plaintiff or any other one concerning WhatsApp malware or spyware. Victims of PEGASUS in any European country can ask to the President of the Council of European Prosecutors (CCPE) who publicly said: "The rule of law and the proper functioning of democracies depend on independent and efficient legal systems that ensure access to justice for all. Only an independent and impartial judicial system can provide the basis for the fair and just resolution of legal disputes. Proper performance of the distinct but complementary roles of judges and prosecutors is a necessary guarantee for the fair, impartial and effective administration of justice. Judges and public prosecutors must both therefore enjoy independence in respect of their functions since both of them ensure, at all stages of the proceedings, that individual rights and freedoms are guaranteed, public order is protected and equality before the law is fully respected".

Please do not hesitate to contact me for further information about our approaches to PEGASUS problems, risks and damages considering this document with 18 pages at www.miguelgallardo.es/whatsapp-pegasus.pdf

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

PEGASUS and NSO Group cellular spying

Document published at www.cita.es/pegasus.pdf

From Madrid, Spain, Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA, is expert witnessing for Courts of Law on Pegasus, a spyware for governments improving commercial products like FLEXISPY Mobile Spy Spy Phone that can be installed on devices running some versions of iOS, Apple's mobile operating system, as well on devices running Android. It was developed by the Israeli cyberarms firm, NSO Group. Secret services are very aware of this kind of spyware risks and illegal advantages for Government surveillance activities. If no judge explicitly allow previously each time it is used for a forensic purpose there is serious criminal case no matter who and how used it.

APEDANICA is looking for documented cases no un un of PEGASUS, FLEXISPY Mobile Spy Spy Phone as well as CELLEBRITE systems. For instance, Catalan parliamentary speaker's cellphone was targeted with PEGASUS. Citizen Lab states that 130 activists have been unjustified victims of the NSO program since 2016. A messaging app account belonging to the Crown Prince of Saudi, Mohammed bin Salman, was used to deploy digital spyware on the phone of Jeff Bezos, who is also CEO of Amazon, "in an effort to influence, if not silence" the newspaper's reporting on the Kingdom.

APEDANICA is very pleased to receive and impart information regarding spyware with special attention to already spied victims following Universal Declaration of Human Rights article 19 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". We include anything not legally forbidden to be published related with agencies like:

National Security Agency NSA ??????? ???????????????? ?????????? in Russian Federation State Security Service General Intelligence and Security Service, military intelligence ADIV/SGRS Coordination Unit for the Threat Assessment OCAD/OCAM in Belgium Nachrichtendienst des Bundes NDB in Switzerland Ministry of State Security MSS in China Reconnaissance General Bureau in North Korea Directorate of Military Intelligence DRM in France Algemene Inlichtingen- en Veiligheidsdienst AIVD in The Netherlands Bundesnachrichtendienst BND in Germany ?????? ???????? ??????????? ??? in Greece Greiningardeild Varnarmálastofnunar Íslands GVMSÍ in Iceland Directorate General of GST Intelligence DGGI in India Ministry of Intelligence VAJA in Iran Inter-Services Intelligence ISI in Pakistan General Intelligence Presidency (GIP) - ????? ??????????? ?????? in Saudi Arabia Federal Security Service FSB ??????????? ?????? ???????????? and Main Intelligence Directorate GRU or Centro Nacional de Inteligencia CNI in Spain

RELEVANT REFERENCES FOR APEDANICA APPROACH

https://news.un.org/en/story/2020/01/1055771

Independent UN rights experts call for 'immediate investigation' into alleged Bezos phone hack by Saudi Arabia David Kaye (left), Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Agnes Callamard, Special Rapporteur on extrajudicial, summary or arbitrary executions.UN Photo/Rick Bajornas/Loey Filipe David Kaye (left), Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Agnes Callamard, Special Rapporteur on extrajudicial, summary or arbitrary executions. 22 January 2020 Human Rights Independent UN rights experts said on Wednesday they were "gravely concerned" over allegations that in 2018, a messaging app account belonging to the Crown Prince of Saudi Arabia was used to hack into The Washington Post owner's mobile phone, calling for an "immediate investigation" by authorities in the United States. The two Special Rapporteurs - who do not speak on behalf of the UN overall, and operate in an independent investigative capacity - said in a statement that they had recently received information suggesting that a WhatsApp account belonging to Crown Prince Mohammed bin Salman was used to deploy digital spyware on the phone of Jeff Bezos, who is also CEO of Amazon, "in an effort to influence, if not silence" the newspaper's reporting on the Kingdom. "The allegations reinforce other reporting pointing to a pattern of targeted surveillance of perceived opponents and those of broader strategic importance to the Saudi authorities, including nationals and non-nationals", said Agnes Callamard, UN Special Rapporteur on summary executions and extrajudicial killings, and David Kaye, UN Special Rapporteur on freedom of expression. "These allegations are relevant as well to ongoing evaluation of claims about the Crown Prince's involvement in the 2018 murder of Saudi and Washington Post journalist, Jamal Khashoggi". They spelled out that the alleged hacking of Mr. Bezos' phone, and those of others, if proven, would be in contravention of fundamental international human rights standards, and demands an "immediate investigation" by US and other relevant authorities, "including investigation of the continuous, multi-year, direct and personal involvement of the Crown Prince in efforts to target perceived opponents". Better controls needed The reported surveillance of Mr. Bezos, allegedly through software developed and marketed by a private company was "transferred to a Government without judicial control of its use", said the experts. If true, they maintained it was "a concrete example of the harms that result from the unconstrained marketing, sale and use of spyware". To protect against its abuse, surveillance through digital means must be "subjected to the most rigorous control", according to the independent experts, including by judicial authorities and national and international export controls. Moreover, they argued that "it underscores the pressing need for a moratorium on the global sale and transfer of private surveillance technology". "The circumstances and timing of the hacking and surveillance of Bezos also strengthen support for further investigation by US and other relevant authorities of the allegations that the Crown Prince ordered, incited, or, at a minimum, was aware of planning for but failed to stop the mission that fatally targeted Mr. Khashoggi in Istanbul", the UN experts stated. 'Clandestine' online campaign While the Kingdom was supposed to be investigating Mr. Khashoggi's murder and prosecuting those responsible, the Rapporteurs said, "it was clandestinely waging a massive online campaign against Mr. Bezos." A 2019 forensic analysis of his iPhone assessed with "medium to high confidence", that it was infiltrated on 1 May 2018 through a video sent from Mohammed bin Salman's WhatsApp account. According to the analysis, the Crown Prince and Mr. Bezos exchanged numbers the month before the alleged hack. The forensic analysis found that within hours of receiving the video from the Crown Prince's account, "an unprecedented exfiltration of data" from the iPhone began. After an initial spike, the unauthorized transfer of data continued undetected for months. The information we have received suggests...an effort to influence, if not silence, The Washington Post's reporting on Saudi Arabia -- UN Experts The analysis also assessed that the intrusion was likely undertaken through a prominent spyware that was identified in other Saudi surveillance cases, the experts said. They added that the allegations were reinforced by separate evidence of Saudi Arabia targeting dissidents and perceived opponents. The Saudi Arabian Embassy in Washington, said on Tuesday night that any suggestion the Kingdom was behind the hacking of Mr. Bezos' phone, "are absurd". Other reported cases The Special Rapporteurs noted that the claims regarding Mr. Bezos' hacked phone are also consistent with the widely reported role of the Crown Prince in allegedly leading a campaign against dissidents and political opponents. They recalled that the iPhone infiltration occurred from May to June in 2018, when the phones of Jamal Khashoggi's associates, Yahya Assiri and Omar Abdulaziz, were also hacked, allegedly using malware called Pegasus. In May 2018, Jamal Khashoggi was a prominent columnist for The Washington Post, writing stories that raised concerns about the Crown Prince's rule. That October, government officials murdered him in the Saudi consulate in Istanbul, Turkey. The newspaper subsequently began covering extensively the disappearance and murder investigation and expanded its reporting on a number of related aspects of the Crown Prince's rule in Saudi Arabia. Breaking it down According to the forensic analysis, after Mr. Bezos' mobile was hacked, the Crown Prince sent him WhatsApp messages in November 2018 and February 2019, "in which he allegedly revealed private and confidential information about the billionaire publisher's personal life that was not available from public sources", said the experts. "During the same period, Mr. Bezos was widely targeted in Saudi social media as an alleged adversary of the Kingdom. This was part of a massive, clandestine online campaign against Mr. Bezos and Amazon, apparently targeting him principally as the owner of The Washington Post." Ms. Callamard and Mr. Kaye "expect to continue investigating the murder of Mr. Khashoggi and the growing role of surveillance in permitting the unaccountable use of spyware to intimidate journalists, human rights defenders and owners of media outlets", concluded the statement released by the UN human rights office, OHCHR. Independent experts' role Special Rapporteurs and independent experts are appointed by the Geneva-based UN Human Rights Council to examine and report back on a specific human rights theme or a country situation. The positions are honorary and the experts are not UN staff, nor are they paid for their work.

https://www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/

ISRAEL AND OCCUPIED PALESTINIAN TERRITORIES HUMAN RIGHTS DEFENDERS AND ACTIVISTS SHARE Facebook Twitter Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence 12 July 2020, 17:41 UTC Today's disgraceful ruling is a cruel blow to people put at risk around the world by NSO Group selling its products to notorious human rights abusers. Danna Ingleton, acting Co-Director of Amnesty Tech A Tel Aviv District Court today rejected an attempt, supported by Amnesty International, which sought to force Israel's Ministry of Defence (MOD) to revoke the security export license of spyware company NSO Group. Danna Ingleton, acting Co-Director of Amnesty Tech, said: "Today's disgraceful ruling is a cruel blow to people put at risk around the world by NSO Group selling its products to notorious human rights abusers. At a moment when NSO and the Israeli MOD should be held accountable for their practices, it is appalling that the court has failed to do so. "NSO Group continues to profit from human rights abuses with impunity. The ruling of the court flies in the face of the mountains of evidence of NSO Group's spyware being used to target human rights defenders from Saudi Arabia to Mexico, including the basis of this case - the targeting of one of our own Amnesty employees. We will continue to do all we can to stop NSO Group's spyware being used to commit human rights abuses. "Until there is transparency around NSO's business practices and guarantees that the Israeli MoD process of granting export licenses is set according to international standards and practices, the company's products will continue to aid in the persecution of activists and the repression of human rights." Background The legal action - brought by members and supporters of Amnesty International Israel and others- comes after evidence has emerged showing how NSO spyware technologies, most notably Pegasus, have been used to target an Amnesty International employee as well as numerous journalists and activists, including in Morocco, Saudi Arabia, Mexico and the UAE. The legal case is supported by Amnesty as part of a joint project with New York University School of Law's Bernstein Institute for Human Rights and the Global Justice Clinic.

https://english.elpais.com/politics/catalonia_independence/2020-07-14/catalan-parliamentary-speakers-cellphone-was-targeted-with-a-spy-program-only-available-to-governments.html

Catalan parliamentary speaker's cellphone was targeted with a spy program only available to governments A Canadian cybersecurity institute that investigated a fault in WhatsApp discovered that Roger Torrent's handset was attacked in 2019 together with a hundred other figures from civil society around the world Catalan parliamentary speaker Roger Torrent. Catalan parliamentary speaker Roger Torrent.TONI ALBIR / EFE JOAQUÍN GIL Madrid - 14 JUL 2020 - 09:30 CEST The cellphone used by the speaker in the Catalan regional parliament, Roger Torrent, was targeted with Pegasus, a spy program developed by an Israeli company named NSO, and which can only be purchased by governments and security forces and used to target crime and terrorism. Torrent's phone was attacked using Pegasus in 2019, according to a joint investigation by EL PAÍS and The Guardian. The intrusion into the handset of the pro-Catalan independence politician, who belongs to the Catalan Republican Left (ERC) party, was possible due to a security fault in the WhatsApp messaging service that, between April and May 2019, could be used to install the NSO spy program in at least 1,400 cellphones across the world. The method for the attack was a missed video call, according to WhatsApp. When you find a Pegasus target, you find the fingerprints of a government CITIZEN LAB RESEARCHER JOHN SCOTT-RAILTON Pegasus took advantage of this weakness to attack Torrent's phone, according to Citizen Lab, a cybersecurity group from the Munk School of Global Affairs and Public Policy at the University of Toronto, which exclusively investigated the fault in the messaging application in 2019. WhatsApp supplied Citizen Lab with the numbers that had been targeted by the Israeli cyberespionage program, among which was that of Torrent, according to these researchers, who publicly revealed the existence of Pegasus. EL PAÍS and The Guardian have had access to a certificate emitted by Citizen Lab that validates the fact that the speaker's phone was attacked with the NSO spyware. "The investigation identified that the number belongs to Mr Roger Torrent," the analysis states. The document explains that the attackers resorted to a missed WhatsApp call "that did not require a response" to target the politician's phone, and it contains "ample evidence that could establish that Torrent was monitored." Torrent's phone figures on a list of a hundred or so cases across the world that were compiled by Citizen Lab of "representatives of civil society" who were indiscriminately attacked via the WhatsApp vulnerability, according to the Canadian institution. Citizen Lab states that 130 activists have been unjustified victims of the NSO program since 2016. Pegasus permits conversations to be listened to, messages read, access to the phone's memory, screenshots to be taken, browsing history to be tracked and for remote access of the device's microphone and camera. This opens the door for the program to listen to the ambient sound in a room if a phone has been infected. The system even allows for encrypted messages and voice calls to be recorded, according to the Canadian experts. In 2018, Pegasus was being used in 45 countries, targeting activists in Bahrain, Kazakhstan, Saudi Arabia, the United Arab Emirates and Mexico The researchers connected the mysterious disappearance of WhatsApp messages from Torrent's cellphone in 2019 with an indication that the phone "could have been manipulated by a third party and infected." And while they cannot identify who ordered the attack, they point out that the Israeli firm that created Pegasus "exclusively sells its products to governments." This fact is confirmed by NSO on its website, where it presents its services as solutions for the armed forces and the police to combat crime. While Torrent's cellphone was targeted by Pegasus, in 2019, the parliamentary speaker took part in dozens of political meetings and also appeared as a witness in Spain's Supreme Court during the trial of the politicians and civil leaders who were involved in the 2017 independence drive in the Catalonia region, which saw an illegal referendum on secession from Spain held in October of that year. Among the sentences handed down by the court, Carme Forcadell, Torrent's predecessor as speaker in the regional parliament, was given 11-and-a-half years in jail for the offense of sedition. In May 2019, when he was being targeted with Pegasus, Torrent took part in a meeting in Strasbourg with the Council of Europe Commissioner for Human Rights, Dunja Mijatvic. "I noticed strange things," Torrent explains. "WhatsApp messages and chat histories would be deleted. It didn't happen to the people around me." The politician also says that he received "strange" SMS messages in 2019. Torrent says that he sees the hand of the "Spanish state" behind the Pegasus attack. "The government has no evidence that the speaker of the Catalan parliament, Roger Torrent [...] [has] been the targets of hacking via their mobiles," says a spokesperson from the Spanish government, who points out that any monitoring of communications requires a court order. A spokesperson from the CNI, Spain's intelligence services, says that the organization acts "in full accordance with the legal system, and with absolute respect for the applicable laws." The same spokesperson adds that the actions of the secret service are supervised by a magistrate from the Supreme Court. EL PAÍS and The Guardian have unsuccessfully tried to obtain the versions of the Civil Guard, the National Police and the Interior Ministry as to what happened. Citizen Lab recognizes the difficulty of proving the reach of the cyber attack on Torrent's cellphone, given that, as it indicates, the NSO programs "have an erasing system on the devices." "When you find a Pegasus target, you find the fingerprints of a government," says the researcher from this group, John Scott-Railton. We can confirm that Torrent's telephone was targeted. However, additional investigation would be necessary to confirm that the phone was hacked CITIZEN LAB RESEARCHER JOHN SCOTT-RAILTON According to the expert, "we can confirm that [Torrent's] telephone was targeted. However, additional investigation would be necessary to confirm that the phone was hacked. At this time we have no reason to believe that it wasn't." After being informed about the issue by this newspaper, Torrent's team got in touch last Thursday with Scott-Railton. "They gave us the cellphone of the parliamentary speaker without us having asked for it and they said that it was among those attacked by Pegasus," a spokesperson for the politician explains. "Was the infection successful? [Citizen Lab researcher John] Scott-Railton believes so because Torrent's WhatsApp messages in 2019 were erased, which is one of the effects of Pegasus." Controlled by the London-based fund Novalpina Capital, NSO says that it has a policy for the investigation of the improper use of its systems. NSO has refused to clarify if Spain is among its clients. "Due to confidentiality agreements, we cannot confirm which authorities use our technology," the company replied via email. The firm has said that it will begin an investigation "if it is proved"

that its products were used improperly in Spain. The Israeli company has distanced itself in the United States' courts from the improper use of its spy program. The firm attributes this responsibility to its clients, the governments who acquire its products. "If anyone installed Pegasus on any alleged 'target devices' it was not [the] defendants [NSO Group]. It would have been an agency of a sovereign government," the company stated as a defense in a lawsuit that it is involved in with WhatsApp. The messaging application reported NSO in October of last year for using its platform to infect the cellphones of activists and diplomats around the world with Pegasus. There is no evidence that Spain's security forces are clients of NSO. The National Police and the CNI did hire their main competitor, Hacking Team from Italy, until at least 2015. This emerged after 400 gigabytes of internal emails from this company were stolen from its servers after they themselves were hacked. In 2018, Pegasus was being used in 45 countries, according to Citizen Lab, targeting activists in Bahrain, Kazakhstan, Saudi Arabia, the United Arab Emirates and Mexico. The cellphones of 25 Mexican politicians, activists and reporters, including the journalists Carmen de Aristegui (Aristegui Noticias), Andrés Villareal and Ismael Bojórquez (Río Doce) and Carlos Loret de Mola (Televisa) were targeted in 2019. As were three members of the organization Mexicans Against Corruption and Impunity, while the leaders of the National Action Party (PAN) Ricardo Anaya and Fernando Rodríguez Noval were also monitored. Omar Radi, a 33-year-old Moroccan journalist, also saw his phone infected by Pegasus after he criticized a judge. OTHER VICTIMS OF PEGASUS As well as Catalan speaker Roger Torrent, Pegasus also targeted the cellphone of Anna Gabriel, a former deputy in the Catalan parliament for the anti-capitalist CUP party, and her lawyer, Olivier Peter. Gabriel fled Spain in 2018 and traveled to Switzerland to avoid testifying before Spanish Supreme Court Judge Pablo Llarena over allegations of rebellion, misappropriation of public funds and sedition in connection to her role in the 2017 Catalan breakaway bid. "[Gabriel] received a WhatsApp notification that told her that her cellphone could have been hacked," explained Peter, alluding to a vulnerability the messaging service suffered between April and May in 2019, which was later fixed. "If the hack is confirmed and we have more information, action will be taken," he added. Jordi Domingo, a staff member of the Tarragona provincial government, was another victim of Pegasus, according to the investigation from EL PAÍS and The Guardian. "That's right. The investigator from Citizen Lab, John Scott, called me last October to tell me that my cellphone was hacked before 2019," said Domingo, who is also a member of the Asamblea Nacional Catalana (ANC) and the separatist Catalan European Democratic Party (PdeCAT). Domingo suggested two reasons for why he may have been targeted. "The first is that it was all a mistake. I have the same name as a well-known separatist lawyer. And the second [is] because I asked Barcelona city hall in 2018 for authorization on behalf of the Observatory against Catalanphobia to hold a demonstration. That very day, the police union Jusapol, held a march." According to Domingo, he was not subject to any legal investigation during the time his cellphone was hacked by Pegasus. When asked if he would report the incident, he replied: "Who would I report? I don't know who spied on me." A spokesperson from the Spanish government said that there was "no evidence" that Gabriel and Domingo had been spied on. English version by Simon Hunter.

https://www.theguardian.com/world/2020/jul/14/second-catalan-politician-says-phone-was-targeted-by-spware

Second Catalan politician says phone was targeted by spyware Ernest Maragall revelation set to boost calls for inquiry into possible domestic espionage Stephanie Kirchgaessner, Sam Jones in Madrid and Jennifer Rankin in Brussels Tue 14 Jul 2020 19.02 BSTLast modified on Tue 14 Jul 2020 20.45 BST Shares 130 Ernest Maragall Ernest Maragall said researchers working with WhatsApp told him his phone was targeted in 2019. Photograph: Europa Press News/Getty Images A second prominent member of Catalan's pro-independence movement has revealed he was warned that his mobile phone was targeted using spyware. The development is likely to bolster calls for an investigation into the possible use of hacking technology by Spanish authorities. Ernest Maragall, an MP in the regional parliament and a former member of the European parliament who also served as Catalan foreign minister, told the Guardian and El País that he was alerted by researchers working with WhatsApp that his phone had been targeted last year. A joint investigation by the newspapers revealed on Monday that Roger Torrent, the speaker of the Catalan parliament, was also targeted in 2019, according to researchers at Citizen Lab at the University of Toronto, who have collaborated with WhatsApp. Advertisement "It is terrible," Maragall said. "This is not a surprise. It is just a part of the techniques, of the reality we are living in every day. We are in a situation where judicial actions, policies, security forces, prosecutors, everybody ... is against our movement, our peaceful and democratic movement as citizens here in Catalonia." Torrent and Maragall - as well as two other pro-independence activists - were alerted that they were targeted in April-May 2019, when spyware used by government clients around the world exploited a previous vulnerability in WhatsApp software. The spyware, made by Israel's NSO Group, allows the operator of the hacking tool to access an individual's phone, including emails, calls and text messages. NSO Group has said it has no knowledge or control over how its clients use the spyware. Current and former leaders of Catalonia's pro-independence government have called for an inquiry into what one researcher at Citizen Lab called a "possible case of domestic political espionage" in Europe. Torrent called the reports "extraordinarily serious", adding: "We cannot normalise spying on political dissidence." He said that if the Spanish government knew of the facts in the case "then it would have been complicit in a crime". If it did not, he said, "it would be a very worrying symptom of political negligence and unawareness of illegal practices". Gabriel Rufián, the spokesman in the national parliament for the Catalan Republican Left party, called on Spain's interior minister, Fernando Grande-Marlaska, to "provide explanations over the alleged spying and invasion of privacy against Catalan political leaders by government organisations". The revelations also resonated in the European parliament, where one of the most senior allies of Pedro Sánchez, the Spanish prime minister, called for an investigation into the targeting of Torrent's phone. Juan Fernando López Aguilar, a Spanish Socialist MEP who chairs the European parliament's civil liberties committee said: "Any indication that there might have been an intrusion in the confidentiality of data of European citizens - be it high officials, representatives, or private citizens for that matter - should be thoroughly investigated." In Spain, he said, such investigations are a matter for the public prosecutor. He added that there was "no ground whatsoever to point out the responsibility of any national agency or government [in connection] to that information we have just read of". The Spanish government said it was a legal, rather than political matter, and suggested that Torrent report his concerns to the judicial authorities. "The government has no evidence that the speaker of the Catalan parliament has been the victim of a hack or theft involving his mobile," the government's spokeswoman, María Jesús Montero, told reporters on Tuesday afternoon. "When questions of this nature arise, the procedure is well known: you inform the relevant judicial authorities about the hack or tapping, or the theft from a device, and they can then investigate whether it has happened and under what circumstances. Any mobile phone tapping always requires preliminary judicial authorisation. This isn't something for the government." In a statement, Spain's interior ministry said: "Neither the interior ministry, nor the national police, nor the Guardia Civil have ever had any relationship with the company that developed this program, and, as such, have never contracted its services." It added that the actions of state security forces were always conducted "with the utmost respect for the law". Spain's National Intelligence Centre (CNI) said in a statement that it acted "in full accordance with the legal system, and with absolute respect for the applicable laws" and that its work was overseen by Spain's supreme court. It did not respond to specific questions about the alleged use of "Pegasus" spyware sold by NSO Group. WhatsApp has said that a total of 1,400 users were targeted in the 2019 attack, which is now the subject of a lawsuit by the messaging app against NSO Group. The California company has claimed that 100 members of civil society - including journalists in India, human rights activists in Morocco, diplomats and senior government officials - are alleged to have been affected. NSO Group has denied it has any role in operating its hacking software and has said it has no knowledge of who its government clients target. The company said it operated under "industry-leading governance policies" and that it could not confirm or deny which authorities used its technology because of confidentiality constraints. The company has been critical of Citizen Lab, which has closely researched the use of NSO Group's spyware, and said researchers had failed to "competently address the challenges faced by law enforcement agencies" who need to intercept encrypted communications. NSO Group has said it sells its spyware solely for governments to track terrorists and criminals. López Aguilar, who worked on the European parliament's response to 2013 revelations that the US National Security Agency had hacked the telephone records of millions of people, said all EU member states were bound to follow European law on data privacy, including the General Data Protection Regulation. "Any member states that might have some breach of that European law should be accountable for it, but those reports first of all have to be fully verified. Protection of rights and privacy are of the essence for the consistency of Europe."

https://www.theguardian.com/world/2020/apr/07/nso-group-points-finger-at-state-clients-in-whatsapp-spying-case

NSO Group points finger at state clients in WhatsApp spying case This article is more than 3 months old In court filing, Israeli spyware company says it does not operate technology it provides Stephanie Kirchgaessner in Washington @skirchy Email Tue 7 Apr 2020 18.13 BSTLast modified on Tue 7 Apr 2020 22.14 BST Shares 73 The offices of NSO group, in Herzliya, near Tel Aviv. WhatsApp has accused the company of hacking 1,400 of its users The offices of NSO group, in Herzliya, near Tel Aviv. WhatsApp has accused the company of hacking 1,400 of its users. Photograph: Jack Guez/AFP via Getty Images An Israeli spyware company that has been accused by WhatsApp of hacking 1,400 of its users, including journalists, human rights activists, and diplomatic officials, has blamed its government clients for the alleged abuses, according to court documents. NSO Group - whose technology is reported to have been used against dozens of targets including Pakistani intelligence officials, Indian journalists and exiled Rwandan political activists - also claimed in legal documents that the lawsuit brought against the company by WhatsApp threatened to infringe on its clients' "national security and foreign policy concerns". WhatsApp sues Israeli firm, accusing it of hacking activists' phones Read more NSO Group has never disclosed a full list of its government clients, but research by Citizen Lab, which tracks the use of spyware, has claimed that current and former clients include Saudi Arabia, Bahrain, Kazakhstan, Morocco, Mexico and the United Arab Emirates. WhatsApp, the popular messaging app, filed a lawsuit against NSO Group in October, alleging that the cyberweapons company was behind a series of highly sophisticated attacks that it claimed violated US law in an "unmistakeable pattern of abuse". Among the alleged victims of the hack, which was discovered last April and continued for two weeks until the app's vulnerability was fixed, were 100 human rights activists, lawyers, journalists and academics who were later notified of the alleged intrusion by WhatsApp. Advertisement In its first substantive legal filing in the case, filed last week, NSO hit back at WhatsApp and its parent company, Facebook, which it said were seen by governments as "safe spaces for terrorists and other criminals" who - without NSO's services - could operate "without fear of detection by law enforcement". NSO Group also argued that WhatsApp had "conflated" NSO Group's actions with the actions of NSO's "sovereign customers". While NSO Group licenses its signature spying technology, Pegasus, to government law enforcement and intelligence agencies and assists with "training, setup, and installation", it said it did not operate the technology. "Government customers do that, making all decisions about how to use the technology," NSO said in its legal filing. "If anyone installed Pegasus on any alleged "target devices" it was not [the] defendants [NSO Group]. It would have been an agency of a sovereign government." NSO Group claimed that to challenge such conduct, WhatsApp would have to declare the "sovereign acts" of those governments to be illegal. "For that reason," the company said in the filing, "permitting this litigation to proceed would infringe critical national security and foreign policy concerns of sovereign governments". The company also highlighted the role it claimed the Israeli government played in its review of NSO Group's business. The Israeli ministry of defence, NSO Group said, could have access to information about NSO Group's customers and "their intended use of Pegasus technology". In a statement, WhatsApp said NSO Group was attempting to "avoid responsibility" and questioned the accuracy of some of the company's claims, including an allegation in the legal filing that Facebook had wanted to procure some of NSO Group's technology in 2017. In a sworn statement filed to the court, Shalev Hulio, an NSO Group co-founder, said that NSO had been approached by two Facebook representatives in October 2017 and asked about the right to "certain capabilities of Pegasus", which the representatives had suggested could be used to help monitor users on Apple devices. NSO Group declined to comment to the Guardian's questions about the alleged meeting between Facebook and NSO, and said it would not reveal the identity of the individuals. WhatsApp said the description of the discussions were an "inaccurate representation". It declined to provide further comment.

HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries

B Marczak, J Scott-Railton, S McKune, B Abdul Razzak. - 2018 - tspace.library.utoronto.ca

Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic

version first published in 2018 by the Citizen Lab . This work can be accessed through

https://citizenlab.ca/2018/09/hide- and-seek-tracking-nso-groups-pegasus-spyware-to-operations .

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Shoshana Zuboff. 2019, New York: Public Affairs.

J Sarah Sam - 2020 - Taylor & Francis

. "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries."

https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague

J Scott-Railton, B Marczak, S Anstis, BA Razzak. - 2018 - tspace.library.utoronto.ca

. Table 1. NSO Group Pegasus Exploit Domains Used in this Operation Page 11. 11 . In

September 2018, prior to the publication of another Citizen Lab report on NSO Group's

Pegasus spyware, NSO Group reiterated that it "develops products .

Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel

E Zureik - Middle East Critique, 2020 - Taylor & Francis

. individual privacy. However, after extensive investigation into the NSO's mode of

operation in Mexico, a report concluded there was no evidence that the use of Pegasus

and other NSO products resulted in positive outcomes.

Some references of APEDANICA

Palestinian BDS National Committee BNC

Document published at www.cita.es/anyvision-palestinians.pdf

From Madrid, Spain, Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA, is investigating AnyVision Israel based company and we have seen published this AnyVision | BDS Movement

Boycott AnyVision: Israel's "field-tested" facial recognition surveillance company

The Palestinian BDS National Committee (BNC) calls for boycotting AnyVision, Israel's facial recognition technology firm, due to its irrefutable complicity in Israel's occupation and repression of Palestinians.

August 30, 2019 By: Palestinian BDS National Committee (BNC)

Considering complaints filled by APEDANICA, Spanish privacy authority AEPD investigates AnyVision business and technologies for Mercadona. We shall appreciate any relevant information useful not only for Spain, but also for the European Union. We suggest to read next document

www.europarl.europa.eu/doceo/document/O-9-2020-000018_EN.html

Parliamentary questions O-000018/2020 Question for oral answer to the Commission Rule 136 Manon Aubry, Anne-Sophie Pelletier, Philippe Lamberts, Manuel Bompard, Leila Chaibi, Clara Ponsatí Obiols, Mick Wallace, Idoia Villanueva Ruiz, Konstantinos Arvanitis, Cornelia Ernst, Emmanuel Maurel, David Cormand, Younous Omarjee, Alexandra Geese, Saskia Bricmont, Viktor Uspaskich, Patrick Breyer, Rosa D'Amato, Markéta Gregorová, Aurore Lalucq, Helmut Scholz, Isabella Adinolfi, Marie Toussaint, Henrike Hahn, Martina Michels, Niyazi Kizilyürek, Fabio Massimo Castaldo, Hilde Vautmans, Pierre Larrouturou, Yannick Jadot, Raphaël Glucksmann, Paul Tang, Nora Mebarek, Stelios Kouloglou, Miguel Urbán Crespo, Alexis Georgoulis, Malin Björk, Petra De Sutter, Ernest Urtasun, Anna Cavazzini, Özlem Demirel, Petros Kokkalis, José Gusmão, Marc Botenga, Maite Pagazaurtundúa, Eugenia Rodríguez Palop, Marisa Matias, Helmut Geuking, Benoît Biteau, Gwendoline Delbos-Corfield, Claude Gruffat, Michèle Rivasi, Caroline Roose Subject: Facial recognition and identification in publicly accessible spaces 1. In the context of the preparation of the White Paper on Artificial Intelligence and the Strategy for Europe - Fit for the Digital Age, does the Commission consider the deployment of facial recognition and/or facial identification systems in publicly accessible spaces by Member States to be inconsistent with Article 9(1) and 9(2)(g) of the General Data Protection Regulation (GDPR) - since it does not meet the requirement of being 'necessary for reasons of substantial public interest' - and Articles 4(1), 8(1) and 10 of the Law Enforcement Directive? 2. Does the Commission identify risks of violations of fundamental rights posed by the deployment of facial recognition and/or facial identification systems in publicly accessible spaces by Member States? 3. If so, is the Commission, as guardian of the treaties, considering banning such practices and/or launching infringement procedures against Member States? Submitted: 01/03/2020

APEDANICA shall be pleased to cooperate with anybody interested in that European Parliamentary question and the next 9 pages in Spanish.

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Nancy Pelosi Speaker of the House of Representatives

Open letter published at www.cita.es/nancy-pelosi-donald-trump.pdf

Dear Madam, Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA from Madrid, Spain, is concerned regarding evidences on CORONAVIRUS COVID-19 pandemic responsibility at the World Health Organisation WHO as well as the United States Intelligence best sources. "President Donald J. Trump Is Demanding Accountability From the World Health Organization" as we can read at

https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-demanding-accountability-world-health-organization/

something widely approved by Europe and Spanish speaking countries.

However, we would like to ask for the same accountability from all public organisations and officials working in any country, including intelligence services of US (Central Intelligence Agency CIA) and Spain (Centro Nacional de Inteligencia CNI), serving in China, or in Italy. Future serious investigations of public responsibility will require most relevant data and metadata, now in computers and international communications in order to evidence who firstly knew what was done with epidemiology sensitive information. Intelligence must be useful for Health authorities, but not for illegal business opportunities, from officials to speculators.

In Spain and Spanish speaking countries APEDANICA has already recommended to preserve every shred of evidence and documents from public servers in China and Italy, as well as stock market records. We suggest to focus Justice and political attention on data or metadata from US Embassy in China to White House since 2019 until current date.

Any official source in China can be relevant for the best intelligence on what was occuring, who knew it, and what was done with data and metadata sensitive information before and after the pandemic was declared by World Health Organisation WHO. Very few authorities can access the computer documents, emails and smartphones data and metadata. We will be obliged if the US Speaker of the House of Representatives could find the best procedure to obtain and preserve the evidence that President Donald Trump supposedly knew, and when he was aware of the real pandemic risk, as well as any illegal business profit made from privileged information, including any stock market illegal speculation. With a view to assist with enquiries we attach 40 pages in this PDF, asking for your acknowledgement of receipt soon.

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Attorney General Freedom of Information Act FOIA

published at www.cita.es/coronavirus-attorney-general.pdf

Spanish non-for-profit Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA (founded in 1992) asks for information on any plaintiff or relevant data or references for expert witnessing and forensic purposes. For instance, right now we are looking for documents about CORONAVIRUS COVID-19 related plaintiffs, in any country or any language, as well as any record, in any Attorney General official files, that can be useful in any Court of Law. We have read this: "On my watch, we will not tolerate schemes or frauds designed to turn large profits by exploiting people's health concerns" said New York Attorney General James at https://www.blackstarnews.com/ny-watch/news/new-york-attorney-general-james-price-gouging-during-coronavirus-crisis

Moreover, APEDANICA is seriously concerned about massive data espionage by companies, like Google (Alphabet), and what have been published about "Project Nightingale" or with the Federal inquiry at

https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867

So, considering Freedom of Information Act 1982 (FOI Act) and any other US Law useful for our request to the Attorney General, we ask for:

1º Any record in any file related with CORONAVIRUS COVID-19

2º Any record related with Google and Health data protection and risks, as well as any technology big company with access to Health metadata like "Project Nightingale", if the attorney general is already aware of.

3º Any record that could be related with schemes or frauds designed to turn large profits by exploiting people´s health concerns

APEDANICA shall be pleased to be useful for any official or investigator and we shall do our best to share our concerns and relevant information with experts from all over the World. In order to explain our approach to CORONAVIRUS COVID-19 and "Project Nightingale" we attach some documents already known by World Health Organization WHO representatives and epidemiology experts in several countries, while we work by WhatsApp Groups with many people that share our interest and Philosophy beyond our official records and files request. Please help us to be useful and do not hesitate to contact me to help you to find the records, because we are sure that attorneys and judges need them too.

Google Sued in Spain Over Data Collecting - The New York ...

www.nytimes.com > technology

18 ago. 2010 - "We are dedicating a lot of our time to finding a solution so that users ... Spanish association of Internet users, whose acronym is Apedanica, .

Spain investigates Google Street View wi-fi snooping - BBC.com

www.bbc.com > news > technology...

17 ago. 2010 - It is in response to a complaint by a privacy watchdog called Apedanica. The Google representative has been summoned to explain what data ...

Investigations of Google Street View - EPIC

epic.org > privacy > streetview

Unknown: Street View cars have gathered data from at least some locations, but ... as Internet Giant Calls Incidents "Accident", Gabriella Hold, Prague Post, May 26, ... In the complaint, APEDANICA president Miguel Gallardo rejects Google's .

[PDF] ????????????? ??????????? ???????? ?????? ?? ?????????? ??????? ? ?????????? ????????????? ???????????

?? ?????? - ?????. ua, 2016 - irbis-nbuv.gov.ua

. 10. Asociación para la Prevención y Estudios de Delitos, Abusos y Negligencias

en Informática y Comunicaciones Avanzadas (APEDANICA) [??????????? ??????].-

??- ??? ???????: http://www.cita.es/apedanica/ 11. United .

Dr. (PhD) Miguel Á. Gallardo, Tel. +34 902998352

www.cita.es > fcc-complaint

APEDANICA now ask for FCC attention to some very dangerous and maybe criminal ... Hiperenlaces en www.cita.es/flexispy y www.miguelgallardo.es/flexispy.pdf ... kind of espionage under Freedom of Information Act (FOIA) as soon as possible. This complaint can be forwarded to any authority in any country and we keep ...

FEDERAL COMMUNICATIONS COMMISSION FCC - CITA

19 nov. 2018 - Complaint against Twitter Inc. SPOOFING in English and Spanish ... APEDANICA asks to FCC, under FOIA , any and all information about.

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

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

THIS DOCUMENT MUST BE KNOWN, AT LEAST, BY

Austria

Österreichische Datenschutzbehörde

Barichgasse 40-42

1030 Wien

Tel. +43 1 52152 2550

email: dsb@dsb.gv.at

Website: http://www.dsb.gv.at/

Member: Dr Andrea JELINEK, Director

Belgium

Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)

Rue de la Presse 35 - Drukpersstraat 35

1000 Bruxelles - Brussel

Tel. +32 2 274 48 00

Fax +32 2 274 48 35

email: contact@apd-gba.be

Website: https://www.autoriteprotectiondonnees.be/ - https://www.gegevensbeschermingsautoriteit.be/

Member: Mr David Stevens, President

Bulgaria

Commission for Personal Data Protection

2, Prof. Tsvetan Lazarov blvd.

Sofia 1592

Tel. + 359 2 915 3580

Fax +359 2 915 3525

email: kzld@cpdp.bg

Website: https://www.cpdp.bg/

Member: Mr Ventsislav KARADJOV, Chairman of the Commission for Personal Data Protection

Croatia

Croatian Personal Data Protection Agency

Selska Cesta 136

10000 Zagreb

Tel. +385 1 4609 000

Fax +385 1 4609 099

email: azop@azop.hr

Website: http://www.azop.hr/

Member: Mr Zdravko Vukic, Director

Cyprus

Commissioner for Personal Data Protection

1 Iasonos Street,

1082 Nicosia

P.O. Box 23378, CY-1682 Nicosia

Tel. +357 22 818 456

Fax +357 22 304 565

email: commissioner@dataprotection.gov.cy

Website: http://www.dataprotection.gov.cy/

Member: Ms Irene LOIZIDOU NIKOLAIDOU, Commissioner for Personal Data Protection

Czech Republic

Office for Personal Data Protection

Pplk. Sochora 27

170 00 Prague 7

Tel. +420 234 665 111

Fax +420 234 665 444

email: posta@uoou.cz

Website: http://www.uoou.cz/

Member: Ms Ivana JANU, President

Denmark

Datatilsynet

Carl Jacobsens Vej 35

2500 Valby

Tel. +45 33 1932 00

Fax +45 33 19 32 18

email: dt@datatilsynet.dk

Website: http://www.datatilsynet.dk/

Member: Ms Cristina Angela GULISANO, Director

Estonia

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)

Tatari 39

10134 Tallinn

Tel. +372 6828 712

email: info@aki.ee

Website: http://www.aki.ee/

Member: Ms Pille Lehis, Director General

European Data Protection Supervisor

Rue Wiertz 60

1047 Bruxelles/Brussel

Office: Rue Montoyer 30, 6th floor

Tel. +32 2 283 19 00

Fax +32 2 283 19 50

email: edps@edps.europa.eu

Website: http://www.edps.europa.eu/EDPSWEB/

Member: Mr Wojciech Wiewiórowski, European Data Protection Supervisor

Finland

Office of the Data Protection Ombudsman

P.O. Box 800

FI-00531 Helsinki

Tel. +358 29 56 66700

Fax +358 29 56 66735

email: tietosuoja@om.fi

Website: http://www.tietosuoja.fi/en/

Member: Mr Reijo AARNIO, Ombudsman

France

Commission Nationale de l'Informatique et des Libertés - CNIL

3 Place de Fontenoy

TSA 80715 - 75334 Paris, Cedex 07

Tel. +33 1 53 73 22 22

Fax +33 1 53 73 22 00

contact: https://www.cnil.fr/en/contact-cnil

Website: http://www.cnil.fr/

Member: Ms Marie-Laure DENIS, President of CNIL

Germany

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Graurheindorfer Straße 153

53117 Bonn

Tel.: +49 228 997799 0

Fax: +49 228 997799 5550

email: poststelle@bfdi.bund.de

Website: http://www.bfdi.bund.de/

Member and joint representative: Mr Prof. Ulrich KELBER, The Federal Commissioner for Data Protection and Freedom of Information

The competence for complaints is split among different data protection supervisory authorities in Germany.

Competent authorities can be identified according to the list provided under www.bfdi.bund.de/anschriften.

Greece

Hellenic Data Protection Authority

Kifisias Av. 1-3, PC 11523

Ampelokipi Athens

Tel. +30 210 6475 600

Fax +30 210 6475 628

email: contact@dpa.gr

Website: http://www.dpa.gr/

Member: Mr Konstantinos Menoudakos, President of the Hellenic Data Protection Authority

Hungary

Hungarian National Authority for Data Protection and Freedom of Information

Szilágyi Erzsébet fasor 22/C

H-1125 Budapest

Tel. +36 1 3911 400

email: privacy@naih.hu

Website: http://www.naih.hu/

Member: Dr Attila PÉTERFALVI, President of the National Authority for Data Protection and Freedom of Information

Ireland

Data Protection Commission

21 Fitzwilliam Square

Dublin 2

D02 RD28

Ireland

Tel. +353 76 110 4800

email: info@dataprotection.ie

Website: http://www.dataprotection.ie/

Member: Ms Helen DIXON, Data Protection Commissioner

Italy

Garante per la protezione dei dati personali

Piazza Venezia, 11

00187 Roma

Tel. +39 06 69677 1

Fax +39 06 69677 785

email: protocollo@gpdp.it

Website: http://www.garanteprivacy.it/

Member: Mr Antonello SORO, President of Garante per la protezione dei dati personali

Latvia

Data State Inspectorate

Blaumana str. 11/13-15

1011 Riga

Tel. +371 6722 3131

Fax +371 6722 3556

email: info@dvi.gov.lv

Website: http://www.dvi.gov.lv/

Member: Ms Jekaterina Macuka, Director of Data State Inspectorate

Lithuania

State Data Protection Inspectorate

L. Sapiegos str. 17

LT-10312 Vilnius

Tel. +370 5 271 2804 / +370 5 279 1445

Fax +370 5 261 9494

email: ada@ada.lt

Website: http://www.ada.lt/

Member: Mr Raimondas Andrijauskas, Director of the State Data Protection Inspectorate

Luxembourg

Commission Nationale pour la Protection des Données

15, Boulevard du Jazz

L-4370 Belvaux

Tel. +352 2610 60 1

Fax +352 2610 60 6099

email: info@cnpd.lu

Website: http://www.cnpd.lu/

Member: Ms Tine A. LARSEN, President of the Commission Nationale pour la Protection des Données

Malta

Office of the Information and Data Protection Commissioner

Second Floor, Airways House

High Street, Sliema SLM 1549

Tel. +356 2328 7100

Fax +356 2328 7198

email: idpc.info@idpc.org.mt

Website: http://www.idpc.org.mt/

Member: Mr Saviour CACHIA, Information and Data Protection Commissioner

Netherlands

Autoriteit Persoonsgegevens

Bezuidenhoutseweg 30

P.O. Box 93374

2509 AJ Den Haag/The Hague

Tel. +31 70 888 8500

Fax +31 70 888 8501

Website: https://autoriteitpersoonsgegevens.nl/nl

Member: Mr Aleid WOLFSEN, Chairman of the Autoriteit Persoonsgegevens

Poland

Urzad Ochrony Danych Osobowych (Personal Data Protection Office)

ul. Stawki 2

00-193 Warsaw

Tel. +48 22 531 03 00

Fax +48 22 531 03 01

email: kancelaria@uodo.gov.pl; zwme@uodo.gov.pl

Website: https://uodo.gov.pl/

Member: Mr Jan NOWAK, President of the Personal Data Protection Office

Portugal

Comissão Nacional de Protecção de Dados - CNPD

Av. D. Carlos I, 134, 1º

1200-651 Lisboa

Tel. +351 21 392 84 00

Fax +351 21 397 68 32

email: geral@cnpd.pt

Website: http://www.cnpd.pt/

Member: Ms Filipa CALVÃO, President, Comissão Nacional de Protecção de Dados

Romania

The National Supervisory Authority for Personal Data Processing

B-dul Magheru 28-30

Sector 1, BUCURESTI

Tel. +40 31 805 9211

Fax +40 31 805 9602

email: anspdcp@dataprotection.ro

Website: http://www.dataprotection.ro/

Member: Ms Ancuta Gianina OPRE, President of the National Supervisory Authority for Personal Data Processing

Slovakia

Office for Personal Data Protection of the Slovak Republic

Hranicná 12

820 07 Bratislava 27

Tel.: + 421 2 32 31 32 14

Fax: + 421 2 32 31 32 34

email: statny.dozor@pdp.gov.sk

Website: http://www.dataprotection.gov.sk/

Slovenia

Information Commissioner of the Republic of Slovenia

Dunajska 22

1000 Ljubljana

Tel. +386 1 230 9730

Fax +386 1 230 9778

email: gp.ip@ip-rs.si

Website: https://www.ip-rs.si/

Member: Ms Mojca PRELESNIK, Information Commissioner of the Republic of Slovenia

Spain

Agencia Española de Protección de Datos (AEPD)

C/Jorge Juan, 6

28001 Madrid

Tel. +34 91 266 3517

Fax +34 91 455 5699

email: internacional@aepd.es

Website: https://www.aepd.es/

Member : Ms María del Mar España Martí, Director of the Spanish Data Protection Agency

Sweden

Datainspektionen

Drottninggatan 29

5th Floor

Box 8114

104 20 Stockholm

Tel. +46 8 657 6100

Fax +46 8 652 8652

email: datainspektionen@datainspektionen.se

Website: http://www.datainspektionen.se/

Member: Ms Lena Lindgren Schelin, Director General of the Data Inspection Board

In accordance with the European Economic Area (EEA) agreement, as from 20 July 2018, the EEA countries, Iceland, Lichtenstein, Norway, became members of the Board without voting right and without the right to be elected as chair and vice-chair, for GDPR related matters (see the EEA fact sheet)

Iceland

Persónuvernd

Rauðarárstígur 10

105 Reykjavík

Tel: +354 510 9600

email: postur@dpa.is

Website: https://www.personuvernd.is or https://www.dpa.is

Ms Helga Þórisdóttir, Commissioner

Liechtenstein

Data Protection Authority, Principality of Liechtenstein

Städtle 38

9490 Vaduz

Principality of Liechtenstein

Tel. +423 236 6090

email: info.dss@llv.li

Website: https://www.datenschutzstelle.li

Member: Dr Marie-Louise Gächter, Commissioner

Norway

Datatilsynet

Tollbugata 3

0152 Oslo

Tel +47 22 39 69 00

email: postkasse@datatilsynet.no

Website: www.datatilsynet.no

Member: Mr Bjørn Erik THON, Director-General

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

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

Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños http://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés http://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
http://cita.es/error-apedanica.jpg
http://cita.es/justicia-tramposa.jpg
http://cita.es/justicia-apedanica.jpg
y 1 documento oficial
www.cita.es/apedanica.pdf

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños https://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés https://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
https://cita.es/error-apedanica.jpg
https://cita.es/justicia-tramposa.jpg
https://cita.es/justicia-apedanica.jpg
y 1 documento oficial
https://www.cita.es/apedanica.pdf

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños https://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés https://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
https://cita.es/error-apedanica.jpg
https://cita.es/justicia-tramposa.jpg
https://cita.es/justicia-apedanica.jpg
y 1 documento oficial
https://www.cita.es/apedanica.pdf

3 ANEXOS en PDF
https://www.miguelgallardo.es/pegasus-policial.pdf
https://cita.es/pegasus-policial-noticia.pdf
https://cita.es/pegasus-policial-aepd.pdf
SOLICITANDO PRONTO ACUSE DE RECIBO DE LOS 3 ANEXOS

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños https://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés https://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
https://cita.es/error-apedanica.jpg
https://cita.es/justicia-tramposa.jpg
https://cita.es/justicia-apedanica.jpg
y 1 documento oficial
https://www.cita.es/apedanica.pdf

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños https://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés https://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
https://cita.es/error-apedanica.jpg
https://cita.es/justicia-tramposa.jpg
https://cita.es/justicia-apedanica.jpg
y 1 documento oficial
https://www.cita.es/apedanica.pdf

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños https://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés https://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
https://cita.es/error-apedanica.jpg
https://cita.es/justicia-tramposa.jpg
https://cita.es/justicia-apedanica.jpg
y 1 documento oficial
https://www.cita.es/apedanica.pdf

--
@APEDANICA Tel. (+34) 902998352
Estamos buscando financiación para 2 estudios
Uno para niños https://www.cita.es/lactantes-laboratorio.pdf
y otro de adultos en inglés https://www.cita.es/fcc-complaint
APEDANICA se presenta en 3 imágenes
https://cita.es/error-apedanica.jpg
https://cita.es/justicia-tramposa.jpg
https://cita.es/justicia-apedanica.jpg
y 1 documento oficial
https://www.cita.es/apedanica.pdf

1 ANEXO en PDF de 6 páginas
https://www.miguelgallardo.es/gustavo-petro.pdf
SOLICITANDO PRONTO ACUSE DEL ANEXO

Dr. (PhD) Ing. Miguel Gallardo perito judicial Tel. (+34) 902998352
Mi CV está en https://www.miguelgallardo.es/cv.pdf
Para seguirme https://twitter.com/miguelgallardo
Presido https://twitter.com/APEDANICA
https://www.cita.es/apedanica.pdf

Resolución 692 del 29 de abril de 2022 expedida por el Ministerio de Salud y Protección Social y sus modificaciones.
Principales medidas de bioseguridad:

* Lávese las manos frecuentemente.
* Evite aglomeraciones en espacios abiertos y cerrados.
* Use correctamente el tapabocas cubriendo nariz y boca.
* Siempre que sea posible mantenga una ventilación adecuada.