Defensora del Pueblo, Excma. Sra. Dª Soledad Becerril Bustamante por **hiperenlaces** en **www.cita.es/defensora-del-pueblo** y **www.miguelgallardo.es/defensora-del-pueblo.pdf**

Considerando los artículos 9 y 10 de la LEY ORGÁNICA 3/1981, DE 6 DE ABRIL, como mejor proceda ponemos en su conocimiento que los **teléfonos móviles (smartphones) de detenidos están siendo inspeccionados y su contenido duplicado en Comisarías de Policía** sin aviso ni permiso ni ninguna garantía técnica o jurídica para el propietario del smartphone registrado por funcionarios de Policía. **En pocos minutos todo el contenido del smartphone se extrae y se utiliza sin autorización judicial ni consentimiento ni conocimiento del detenido.**

El espionaje electrónico siempre resulta difícil de detectar y más aún de probar judicialmente si los **funcionarios de Policía niegan los hechos y encubren a sus responsables**. Estamos trabajando en tecnologías que evidencien la intrusión ilícita, agresivas pero en defensa propia.

Obviamente, con orden judicial, o bien con el consentimiento del detenido y unas adecuadas garantías, el registro de smartphones puede ser muy útil para la investigación policial, pero **si se hace ilegalmente se corre el riesgo de que se anulen las actuaciones posibilitando que los peores criminales queden impunes por este tipo de prácticas policiales ilegales**.

Es conocida la marca del fabricante "Cellebrite" que se jacta de suministrar a policías diversos sistemas para la extracción de datos de smartphones, incluyendo lo ya borrado, Sin embargo, no aparece en ninguna adjudicación publicada en el Boletín Oficial del Estado (BOE), por lo que considerando las evidencias de su uso policial, es también preocupante la falta de transparencia no solamente por razones económicas, sino también porque algunos equipos "Cellebrite" parecen disponer de un **sistema de "mantenimiento remoto" que posibilita el "espionaje del espionaje" y la dependencia de la seguridad del Estado hacia empresas extranjeras**.

Hemos tratado de interesar al **Consejo General de la Abogacía Española (CGAE)** y a varios responsables de la asistencia a detenidos en Comisarías obteniendo un preocupante silencio. También hemos denunciado a la **Agencia Española de Protección de Datos** y **Comisión Europea** (a la que recurrimos por tercera vez). Aquí entendemos que nadie mejor que la Defensora del Pueblo para requerir información y garantizar derechos que deberían ser iguales para todos los ciudadanos, incluyendo también al ministro del Interior, secretario de Estado de Seguridad, director de la Policía y comisario de Asuntos Internos, cuyos smartphones no deben tener ni más ni menos seguridad que el de cualquier detenido sin orden judicial. En muchos casos, un sencillo sobre bien precintado es más que suficiente. En otros, hasta los servicios de inteligencia pueden correr serios riesgos si no se racionaliza y civiliza la detención policial y el espionaje masivo tanto de terminales móviles smartphones como sobre el cada vez más inseguro sistema GSM, contra el espíritu y la letra del artículo 18 de la Constitución Española.

Fdo.: Miguel Ángel Gallardo Ortiz, Licenciado en Filosofía, Ingeniero y Criminólogo, perito judicial en criptología forense y telefonía móvil (smartphones) en su propio nombre y derecho y también por CITA y APEDANICA Tel. (+34) 902998352, E-mail: miguel@cita.es
C/ Fernando Poo, 16 Piso 6ºB 28045 Madrid para **www.cita.es/defensora-del-pueblo**
Se adjuntan 7 páginas con documentación e hiperenlaces relevantes en escritos dirigido al **Consejo General de la Abogacía Española (CGAE)**, **Comisión Europea** (3 asuntos distintos por incumplimienrto de derecho europeo) y **Agencia Española de Protección de Datos**

Perito por detenidos al Consejo General de la Abogacía Española CGAE en **hiperenlaces relevantes** www.cita.es/perito-detenidos y www.miguelgallardo.es/perito-detenidos.pdf

Considerando el "**Protocolo de asistencia letrada al detenido**" del CGAE, queremos elevar una inquietud con propuestas para interesar a abogados por los riesgos de los teléfonos móviles **smartphones de detenidos en Comisarías de Policía** en la seguridad de que los letrados más sensibles a esta problemática entenderán la intención y la utilidad de nuestras propuestas.

Sabemos que el Ministerio del Interior ha adquirido, y utiliza sin control ni garantías, sistemas para la extracción total, incluso de la información ya borrada, del **teléfono móvil del detenido en Comisarías de Policía**. Este hecho pone en riesgo no solamente la seguridad jurídica del detenido, sino también derechos fundamentales de todas las personas que antes se hayan relacionado con él por whatsapps o mensajes privados en redes sociales, y en todo caso, las agendas de contactos y listados de llamadas entrantes o salientes posibilitan un inadmisible **espionaje policial contrario a los más elementales derechos y garantías, actualmente**.

No tenemos noticia de que algún detenido haya denunciado el acceso policial indebido a datos de su móvil smartphone, aunque sí **conocemos un singular caso** en el que se han producido dos detenciones que tenían como principal propósito policial la incautación y registro con extracción de copia total del móvil del mismo detenido, las dos veces. También nos hemos dirigido a embajadores y cónsules de países como **Estados Unidos** y **Alemania** cuyos nacionales pueden quedar en mayor indefensión al ser espiados sus móviles en sede policial.

Hemos puesto este problema en conocimiento de la Agencia Española de Protección de Datos y también de la **Comisión Europea** que ya ha iniciado el trámite para analizar si esta práctica policial española es **contraria al Derecho Comunitario Europeo**. En todo caso, pedimos la colaboración de los letrados que asistan a detenidos en Comisaría, o una vez que ya han sido puestos a disposición judicial, pero cuyos teléfonos móviles smartphones han sido incautados el tiempo suficiente como para que se hayan extraído sus datos y metadatos (bastan muy pocos minutos para que un policía adiestrado obtenga una copia total del contenido del smartphone).

Cuando no se pueda evitar esta grave intrusión policial, lo que pericialmente recomendamos es que el detenido ejerza su **derecho a obtener copia íntegra y fedatada por secretario judicial** del contenido total extraído que parece ser que la Policía actualmente guarda, y si se le requiere tiene la obligación de copia al Juzgado de Instrucción, en DVDs fácilmente duplicables.

Agradeceremos al CGAE que se estudie esta inquietud con nuestra propuesta para que la **Comisión Europea** regule los derechos del detenido y las obligaciones de los funcionarios de Policía cuando se incauta temporalmente un teléfono móvil smartphone, y como peritos, estamos a la disposición de los letrados que compartan con nosotros esta inquietud por la que vamos a invitar a deliberar próximamente en el **www.clubfinancierogenova.com** de Madrid.

Fdo.: Miguel Gallardo por CITA y APEDANICA Tel. (+34) 902998352, E-mail: miguel@cita.es
Ingeniero y Criminólogo, perito judicial en criptología forense y telefonía móvil (smartphones)
C/ Fernando Poo, 16 Piso 6ºB 28045 Madrid en www.cita.es/perito-detenidos
Referencias relevantes en las siguientes 5 páginas con 3 procedimientos de denuncia a la **Comisión Europea**, así como en el trabajo de investigación en **www.miguelgallardo.es/policiologia.pdf**

COMISIÓN EUROPEA, DIRECCIÓN GENERAL DE JUSTICIA (denuncias)

Dirección C: Derechos fundamentales y Ciudadanía de la dad C3: Protección de datos y también para el Secretariat of the Art. 29 Working Party ("EL GRUPO") con enlaces en www.cita.es/ce-smartphones y www.miguelgallardo.es/ce-smartphones.pdf

Considerando que "*cualquier persona podrá acusar a un Estado miembro mediante la presentación de una denuncia ante la Comisión, denunciando una medida (legislativa, reglamentaria o administrativa) o una práctica imputables a un Estado miembro que considere contrarias a una disposición o a un principio de Derecho de la Unión Europea*", aquí se **DENUNCIA** que:

1º En España la **Policía** utiliza sistemas para el registro y copiado de teléfonos móviles incautados a **detenidos en Comisaría**. Tenemos documentado, al menos, un caso de registro policial de un móvil iPhone 5 con informe policial aportando 3 DVDs de los que el detenido no tuvo conocimiento hasta varios meses después, por vía judicial. Consideramos que es un derecho fundamental del detenido el saber si su móvil ha sido o no registrado, y cuando sí se haya registrado con toda garantía legal, **debe disponer muy pronto de copia completa de cuanto la Policía obtuvo de su propio móvil**.

2º La Comisión Europea ya conoce la existencia de estos sistemas de espionaje de móviles, al menos, por la pregunta de la eurodiputada Cornelia ERNST de fecha **18.1.12** contestada por la comisaria Anna Cecilia Malmström con fecha **15.2.12** textualmente así: "*Europol currently has two such devices, provided by Cellebrite. Only specifically trained Europol staff may operate them. They are used solely for forensic examination of seized cell phones and are deployed only on request from a competent national authority, in compliance with national legislation*". 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 "smartphone". Obviamente existen otras marcas comerciales, e incluso aplicaciones para conectar por puertos USB o Bluetooth para espiar móviles, pero en esta denuncia señalamos los **adquiridos y empleados por la Policía**.

3º Los denunciantes solicitan a la Comisión Europea que se requiera toda la información sobre los sistemas para el **registro de los teléfonos móviles de los detenidos en comisarías españolas**, incluyendo, al menos, los **protocolos policiales**, los **fundamentos jurídicos**, los **derechos del detenido cuando su móvil ha sido registrado** y también marcas, modelos, coste y especificaciones técnicas de los **equipos adquiridos y empleados por la Policía en España para tal fin**.

Esta denuncia es pública. No requerimos ninguna confidencialidad. Antes al contrario, solicitamos la máxima difusión internacional para los hechos denunciados, y consideramos que, más allá del derecho europeo, al menos, en las Directivas 2002/22, 2002/58 y 2009/136, estos hechos y riesgos afectan a derechos humanos fundamentales amparados por **Resolución 68/167 de Naciones Unidas aprobada por la Asamblea General el 18.12.2013** "***El derecho a la privacidad en la era digital***".

Fdo.: Miguel Gallardo por CITA y APEDANICA Tel. (+34) 902998352, E-mail: miguel@cita.es
Ingeniero y Criminólogo, perito judicial en criptología forense y telefonía móvil (smartphones)
C/ Fernando Poo, 16 Piso 6ºB 28045 Madrid. **Documento en enlace** www.cita.es/ce-smartphones
Agradeceremos el debate y los comentarios en www.twitter.com/miguelencita y **@APEDANICA**

COMISIÓN EUROPEA, DIRECCIÓN GENERAL DE JUSTICIA

Dirección C: Derechos fundamentales y Ciudadanía de la Unión Unidad C3: Protección de datos y también para el Secretariat of the Art. 29 Working Party ("EL GRUPO")

Hiperenlaces que quedarán publicados con la versión definitiva enviada finalmente en www.cita.es/stingray y **www.miguelgallardo.es/stingray.pdf**

Miguel Ángel Gallardo Ortiz, ingeniero, criminólogo, licenciado en Filosofía y diplomado en Altos Estudios Internacionales, perito judicial en informática, telemática, acústica y criptología forense administrador de Cooperación Internacional en Tecnologías Avanzadas (CITA) SLU desde 1996, y presidente de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA), desde 1992, con domicilio en calle Fernando Poo, 16 Piso 6ºB 28045 Madrid, **Tel 902998352 fax 902998379** E-mail: miguel@cita.es
como mejor proceda **DENUNCIA estos comprobables y documentables HECHOS**:

1º La Comisión Europea parece haber financiado proyectos relacionados con intrusiones o espionaje de teléfonos móviles GSM con falsas estaciones base o sistemas IMSI-catchers (**CRO IMSI**) o **StingRay**, y recibió propuestas como "**European Project for Development of Holistic Responses in Policing**" en que participaron, entre otras, las entidades españolas Asociación Suyae, Universidad de Lleida, Universidad Autónoma de Madrid, Policía Municipal de Madrid y Mossos d'Esquadra de Catalunya. Sin embargo, no conocemos ninguna resolución europea, ni proyecto alguno, para garantizar los derechos de los ciudadanos frente a la intrusión de las antenas o estaciones falsas que, actualmente, espían teléfonos móviles GSM masivamente en Europa.

2º Tenemos noticias de la detección de IMSI-catchers en Alemania, Finlandia, Suecia y Noruega que se están investigando por periodistas y medios de comunicación que utilizan sistemas privados como "IMSI-catchers-catchers" capaces de evidenciar anomalías en celdas de la red GSM. En España existen indicios racionales del uso indebido y presuntamente sin autorización de un sistema de interceptación y localización de teléfonos móviles que afectó a numerosos ciudadanos porque no solamente espían al objetivo, sino que también captan los metadatos de los terminales GSM en sus proximidades, así como la identificación de quienes comunican con ellos, ilegalmente.

3º El problema pericial en el que se centran las investigaciones de CITA y APEDANICA ahora mismo consiste en la evidencia para prueba judicial de que una antena o estación base GSM falsa ha sido utilizada, para lo que ya hemos solicitado a un juez que preserve los datos efímeros de las estaciones base como se puede comprender leyendo la **querella con hiperenlaces relevantes** que mantenemos en Internet **www.cita.es/querella-ai y www.miguelgallardo.es/querella-ai.pdf** con la **ampliación detallada** en **www.cita.es/ampliando-ai** y **www.miguelgallardo.es/ampliando-ai.pdf**

4º Las operadoras de telefonía móvil, necesariamente, han de tener responsabilidades y deben garantizar que sus sistemas automáticamente detectan antenas y estaciones base GSM falsas en el mismo momento en el que una de ellas entre en funcionamiento en cualquier punto de la red europea y también deben ser capaces de probar, a efectos judiciales, cuándo y dónde se ha utilizado algo parecido al **StingRay** aportando todos los datos que la Justicia les requiera, inmediatamente.

5º Obviamente, el Derecho de la Unión Europea ha sido violado, al menos, por lo dispuesto en la **DIRECTIVA 2009/136/CE** DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores (que menciona expresamente "***riesgos para la seguridad personal — que puede, por ejemplo, producirse como consecuencia de la revelación de información personal en determinadas circunstancias*** *—, así como los* ***riesgos para el derecho a la intimidad y la protección de los datos personales***" y también dice textualmente que "*se debe establecer una política de seguridad para el tratamiento de los datos personales, a fin de identificar las vulnerabilidades del sistema, y proceder, de manera periódica, a una supervisión y a la adopción de* ***medidas preventivas, correctoras y paliativas***"). ¿Si existen, **cuáles son esas medidas** frente al uso no autorizado de IMSI catchers o **StingRay**?

6º Considerando que "*cualquier persona podrá acusar a un Estado miembro mediante la presentación de una denuncia ante la Comisión, denunciando una medida (legislativa, reglamentaria o administrativa) o una práctica imputables a un Estado miembro que considere contrarias a una disposición o a un principio de Derecho de la Unión Europea. No deberá usted demostrar la existencia de un interés por su parte; tampoco tendrá que probar que tiene un interés principal y directo en la infracción que denuncia. Para que una denuncia sea admisible, es necesario que denuncie una violación del Derecho de la Unión Europea por un Estado miembro; no puede, por tanto, referirse a un litigio privado*", entendemos que esta denuncia no trata de ningún litigio privado, sino del sistemático incumplimiento del Derecho de la Unión Europea cada vez que se utiliza una antena o estación base GSM falsa, impunemente. El criterio correcto es que si un juez autoriza su uso (basta la certificación que pedimos) todo será legal y recurrible, pero si el uso no está autorizado judicialmente, siempre será delictivo, sea quien sea quien la utilice, tanto si son servicios secretos o de inteligencia, como si son criminales organizados quienes lo hacen, porque lamentablemente, en muchas ocasiones, se entremezclan demasiado unos y otros y, en ningún caso, puede permitirse espionaje masivo de telefonía móvil sin autorización judicial previa e instamos a la Comisión Europea a tomar medidas preventivas, correctoras y paliativas, pero también transparentes y garantistas de manera que, a requerimiento de un juez, las operadoras telefónicas inmediatamente aporten la información relevante sobre cualquier anomalía sospechosa en su red.

Los aquí denunciantes autorizan expresamente el uso no confidencial de esta denuncia que nosotros mismos hacemos pública en Internet, como también hicimos con la que mantenemos con **enlaces** en www.cita.es/ce-vodafone y **www.miguelgallardo.es/ce-vodafone.pdf** que con fecha 18.6.15 se nos comunicó el registro **CHAP(2014)01926** por BOULANGER Marie-Hélène sin que tengamos más noticia desde entonces y aquí solicitamos información tanto de ese procedimiento iniciado hace más de 6 meses, como tan inmediata como sea posible sobre el que se inicie por esta nueva denuncia.

Fdo.: Miguel Gallardo por CITA y APEDANICA Tel. (+34) 902998352, E-mail: miguel@cita.es
Hiperenlaces en www.cita.es/stingray y **www.miguelgallardo.es/stingray.pdf**

COMISIÓN EUROPEA, DIRECCIÓN GENERAL DE JUSTICIA

Dirección C: Derechos fundamentales y Ciudadanía de la Unión Unidad C3: Protección de datos y

también para el Secretariat of the Art. 29 Working Party ("EL GRUPO")

Hiperenlaces que quedarán publicados con la versión definitiva enviada finalmente en www.cita.es/ce-vodafone y **www.miguelgallardo.es/ce-vodafone.pdf**

Miguel Ángel Gallardo Ortiz, ingeniero, criminólogo, licenciado en Filosofía y diplomado en Altos Estudios Internacionales, perito judicial en informática, telemática, acústica y criptología forense administrador de Cooperación Internacional en Tecnologías Avanzadas (CITA) SLU desde 1996, y presidente de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA), desde 1992, con domicilio en calle Fernando Poo, 16 Piso 6ºB 28045 Madrid, **Tel 902998352 fax 902998379** E-mail: miguel@cita.es y **cita902998352@gmail.com** como mejor proceda **DENUNCIA este HECHO**:

The Guardian publicó el 6.6.14 el titular "*Vodafone reveals existence of secret wires that allow state surveillance. Wires allow agencies to listen to or record live conversations, in what privacy campaigners are calling a 'nightmare scenario'*" haciendo referencia a informes que hemos puesto en conocimiento de las autoridades españolas según puede leerse en el documento adjunto, pero entendemos que los hechos tienen ámbito europeo y multiplican su complejidad por países con normativas heterogéneas y diversas operadoras que, a diferencia de Vodafone, no informan, o no se conoce si informan, de estos hechos. Según **The Guardian**, que cita a Vodafone por "**Country-by-country disclosure of law enforcement assistance demands**", Italia registra 605,601 intrusiones, Francia 3 y Rumanía prohíbe cualquier publicación al respecto dándose muy diversos resultados en los demás países según las diferentes categorías de intrusiones posibles en Vodafone.

Considerando la Directiva 95/46/CE, Artículo 30 1. El Grupo tendrá por cometido:
a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea; y cualquier otra normativa aplicable según la jurisprudencia del Tribunal de Justicia de la Unión Europea, como mejor proceda solicitamos que se abran los expedientes más adecuados y eficaces, informándonos tanto como sea posible a la mayor brevedad considerando lo expuesto y denunciado en este documento y su adjunto que quedan publicados con **hiperenlaces relevantes** en Internet
www.cita.es/ce-vodafone y **www.miguelgallardo.es/ce-vodafone.pdf**

Referencias anteriores nuestras: www.miguelgallardo.es/facebook.pdf www.miguelgallardo.es/consultando.pdf y www.miguelgallardo.es/respondido.pdf www.cita.es/google.pdf www.cita.es/querella-google www.cita.es/nsa-querella **www.cita.es/nsa-inconstitucinal www.cita.es/reverint www.cita.es/osce y se adjunta** www.cita.es/aepd-vodafone y www.miguelgallardo.es/aepd-vodafone.pdf

A la Agencia Española de Protección de Datos AEPD www.agpd.es

www.cita.es/aepd-vodafone y www.miguelgallardo.es/aepd-vodafone.pdf

Miguel Ángel Gallardo Ortiz, ingeniero, criminólogo, licenciado en Filosofía y diplomado en Altos Estudios Internacionales, perito judicial en informática, telemática, acústica y criptología forense administrador de Cooperación Internacional en Tecnologías Avanzadas (CITA) SLU desde 1996, y presidente de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA), desde 1992, con domicilio en calle Fernando Poo, 16 Piso 6ºB 28045 Madrid, **Tel 902998352 fax 902998379** E-mail: miguel@cita.es y **cita902998352@gmail.com** como mejor proceda **DENUNCIA estos HECHOS**:

1º **Europa Press el 6.6.14** se hace eco de un muy revelador informe de Vodafone disponible en http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html en el que pueden leerse estos datos relativos a intrusiones España:

SPAIN	Lawful Interception	Communications Data
Statistics	24,212 (1)	48,679 (1)
Key Note (1)	**The legal position is unclear regarding whether or not it would l lawful for Vodafone to disclose statistics related to agency an authority lawful interception and communications data demands. W asked the authorities for guidance and have been informed that w can disclose this information.**	

2º Según **Europa Press**, "*El informe determina que en algunos de estos países se pincha directamente las redes de las empresas telefónicas para poder escuchar o almacenar cualquier conversación privada e incluso conocer la localización exacta de los usuarios. En seis de los países en los que opera Vodafone, la ley obliga a las telefónicas a instalar cables que dan acceso directo a la red o permite a las autoridades hacerlo. La empresa no ha querido revelar los nombres de estos países para evitar represalias sobre su personal. Con estos "pinchazos", los organismos estatales se pueden saltar los controles judiciales y las telefónicas en ningún momento saben a qué información acceden las autoridades.* ***En muchos de los países en los que opera Vodafone, incluido España, es ilegal realizar estas escuchas y obtener los datos sobre tráfico de llamadas a menos que antes haya una orden judicial justificada para ello*** *…*". **Por lo tanto, según Vodafone, sin orden judicial se está accediendo actualmente tanto al audio como a datos y metadatos de sus clientes, así como a los de todos los que hayan mantenido alguna relación con ellos**, violando así el espíritu y la letra de la LOPD.

El denunciante y sus representadas CITA y APEDANICA solicitan que la AEPD abra un expediente por estos hechos y que **nos tenga por personados en él como afectados** manteniendo esta denuncia publicada con **hiperenlaces relevantes en Internet** www.cita.es/aepd-vodafone y www.miguelgallardo.es/aepd-vodafone.pdf

A la Agencia Española de Protección de Datos AEPD www.agpd.es

Enlaces en www.cita.es/aepd-smartphones y www.miguelgallardo.es/aepd-smartphones.pdf

Miguel Ángel Gallardo Ortiz, ingeniero, criminólogo, licenciado en Filosofía y diplomado en Altos Estudios Internacionales, perito judicial en informática, telemática, acústica y criptología forense administrador de Cooperación Internacional en Tecnologías Avanzadas (CITA) SLU desde 1996, y presidente de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA), desde 1992, con domicilio en calle Fernando Poo, 16 Piso 6ºB 28045 Madrid, **Tel 902998352 fax 902998379** E-mail: miguel@cita.es y **cita902998352@gmail.com** como mejor proceda **DENUNCIA estos HECHOS**:

1º La Policía está utilizando sistemas para el registro y copiado de teléfonos móviles incautados a **detenidos en Comisaría**. Tenemos documentado, al menos, un caso de registro policial de un móvil iPhone 5 con informe policial aportando 3 DVDs de los que el detenido no tuvo conocimiento hasta varios meses después, por vía judicial. Consideramos que es un derecho fundamental del detenido el saber si su móvil ha sido o no registrado, y cuando sí se haya registrado con toda garantía legal, **debe disponer pronto de copia completa de cuanto la Policía obtuvo de su propio móvil**.

2º La Comisión Europea ya conoce la existencia de **estos sistemas de espionaje de móviles**, al menos, por la pregunta de la eurodiputada Cornelia ERNST de fecha **18.1.12** contestada por la comisaria Anna Cecilia Malmström con fecha **15.2.12** textualmente así: "*Europol currently has two such devices, provided by Cellebrite. Only specifically trained Europol staff may operate them. They are used solely for forensic examination of seized cell phones and are deployed only on request from a competent national authority, in compliance with national legislation*". 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 "smartphone". Obviamente existen otras marcas comerciales, e incluso aplicaciones para conectar por puertos USB o Bluetooth para espiar móviles, pero en esta denuncia señalamos los **adquiridos y empleados por la Policía**.

3º Los denunciantes solicitan a la AEPD que incoe expediente para requerir información sobre los sistemas para el **registro de los teléfonos móviles de los detenidos en comisarías españolas**, incluyendo, al menos, los protocolos policiales, los fundamentos jurídicos, los **derechos del detenido cuando su móvil ha sido registrado** y también marcas, modelos, coste y especificaciones técnicas de los equipos adquiridos y empleados por la Policía para extraer datos de smartphones.

Esta denuncia es pública y no requerimos ninguna confidencialidad. Antes al contrario, solicitamos la máxima difusión internacional para los hechos denunciados, y consideramos que, más allá del derecho europeo, al menos, en las Directivas 2002/22, 2002/58 y 2009/136, estos hechos y riesgos afectan a derechos humanos fundamentales amparados por **Resolución 68/167 de Naciones Unidas aprobada por la Asamblea General el 18.12.2013** "***El derecho a la privacidad en la era digital***".

Fdo.: Miguel Gallardo por CITA y APEDANICA Tel. (+34) 902998352, E-mail: miguel@cita.es
Ingeniero y Criminólogo, perito judicial en criptología forense y telefonía móvil (smartphones)
C/ Fernando Poo, 16 Piso 6º B - 28045 Madrid, aquí por por www.cita.es/aepd-smartphones