

## 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](http://www.cita.es/stingray) y [www.miguelgallardo.es/stingray.pdf](http://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](mailto: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](http://www.cita.es/querella-ai) y [www.miguelgallardo.es/querella-ai.pdf](http://www.miguelgallardo.es/querella-ai.pdf) con la [ampliación detallada](#) en [www.cita.es/ampliando-ai](http://www.cita.es/ampliando-ai) y [www.miguelgallardo.es/ampliando-ai.pdf](http://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 denunciadores 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](http://www.cita.es/ce-vodafone) y [www.miguelgallardo.es/ce-vodafone.pdf](http://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](http://CITA) y [APEDANICA](http://APEDANICA) Tel. (+34) 902998352, E-mail: [miguel@cita.es](mailto:miguel@cita.es)  
**Hiperenlaces** en [www.cita.es/stingray](http://www.cita.es/stingray) y [www.miguelgallardo.es/stingray.pdf](http://www.miguelgallardo.es/stingray.pdf)