HABEAS SMARTPHONE, HABEAS AUDIO Y HABEAS DATA

PROBÁTICA CRIMINALÍSTICA EN TELEFONÍA CELULAR AVANZADA Y SU ESPIONAJE

Dr. e Ing. **Miguel Gallardo**, criptólogo y perito judicial privado en España y Avv. **Achille Campagna**, abogado y notario ejerciente en San Marino / Italia, por **Asociación @APEDANICA** Tel. (+34) 902998352 y E-mail: apedanica.ong@gmail.com

El derecho penal contemporáneo, en la práctica, encuentra sus límites en el enjuiciamiento de lo que puede llegar a ser probado. Los viejos fundamentos teóricos del derecho romano se enfrentan a un nuevo escenario creado por aparatos que caben en el bolsillo y se integran en redes hipercomplejas. Entre Ulpiano o César y Google o Apple, existe una cambiante fenomenología que obliga a replantearse la doctrina aplicable en cada caso en el que un smartphone afecta o es afectado por un conflicto de derechos en los que los esclavos no tienen, o no están autorizados a utilizarlos, mientras que plebeyos con Android y patricios con Apple iPhone libran batallas desiguales en las que de vez en cuando un Espartaco amenaza a la Roma eterna hasta la invasión de los bárbaros.

Las combinaciones de hechos y derechos relacionados con la telefonía móvil o celular son inabarcables, pero en lo que sigue se ofrecerán algunas definiciones intentando dividir categorizando situaciones de hecho en precedentes, bienes, daños y riesgos del derecho penal contemporáneo relacionables con los teléfonos móviles o celulares “smartphones”.

¿Qué es un “smartphone”? Google (y algo sabe de ellos) lo define así:
smartphone, *nombre masculino*
Teléfono celular con pantalla táctil, que permite al usuario conectarse a internet, gestionar cuentas de correo electrónico e instalar otras aplicaciones y recursos a modo de pequeño computador.
sinónimos: teléfono inteligente

Esta definición simplifica una realidad que determina y condiciona la actividad diaria de los profesionales del derecho probablemente más que ningún otro aparato lo haya hecho antes desde la invención de la imprenta de Gutenberg. Como decía Wittgenstein en su Tractatus[1] “lo que puede mostrarse no puede decirse” y cualquier descripción de lo que es o no es un smartphone se ve ridiculizada por obsoleta y simplista en poco tiempo.

¿Qué puede hacer un “smartphone”? Quienes llevan tiempo utilizando uno y exploran sus límites tecnológicos saben que el potencial es inabarcable porque hasta los más expertos se sorprenden por las innovaciones que compiten como aplicaciones (apps) disponibles en las tiendas virtuales, pero en principio, un smartphone puede hacer prácticamente todo lo que puede hacer un ordenador personal, en cualquier lugar y por supuesto, el smartphone, tanto si es básico en uso muy primitivo, como si es de última generación utilizado por un sofisticadísimo hacker, no deja de ser también un teléfono.

---

[1] Tractatus Logico-Philosophicus 4.1212 (English) - kfs
www.kfs.org/jonathan/witt/t41212en.html
4.1212: *What can be shown cannot be said*. Lo que se puede mostrar no se puede decir.

Por lo tanto, todo el derecho informático y telefónico tal y como se les concibe hasta ahora, es parte del derecho de los smartphones, pero su pequeño tamaño, altísima disponibilidad en uso masivo y la creciente complejidad de sus sistemas en red han hecho explotar una casuística y una fenomenología que sorprende sin preparación alguna a los juristas más tecnológicos, en situaciones límite. La integración de audio y video con datos y metadatos en un pequeño aparato que cabe en un bolsillo ha creado un nuevo escenario jurídico y una problemática en la que el perito puede alterar cualquier enjuiciamiento posible.

¿Cuáles son los principales riesgos y oportunidades para el jurista?

El "habeas data" forma parte de las modernas constituciones y se desarrolla en los ordenamientos jurídicos de todos los países, actualmente. El derecho comunitario europeo emite directivas que se transponen a las legislaciones nacionales y el Tribunal de Justicia de la Unión Europea ha dictado muy relevantes sentencias que afectan a los datos personales así como al mercado y a los consumidores intentando protegerles de monopolios u oligopolios y abusos de posiciones dominantes. Sin embargo, la realidad es que existen dos modelos de sistemas que se han impuesto, el elitista cerrado del Apple iPhone y el gran conquistador de industrias y mercados de Google Android. No hay medallas de bronce en unas tecnologías tan competitivas que han extinguido por extenuación a líderes anteriores con productos diferenciados como Nokia (symbian), Blackberry, Motorola y hasta a la mismísima Microsoft. Las guerras de patentes en el más cruel derecho industrial, la competencia más feroz y tramposa crean litigios nunca antes vistos ni imaginados entre Apple, Google, Samsung, Oracle y Microsoft, entre otros grandes monstruos, y de ellos con gobiernos o instituciones supranacionales como la Unión Europea, así como con todo tipo de consumidores y usuarios.

Hasta la más simple de las redes sociales y por supuesto Twitter, FaceBook FB, Google+ G+ y sistemas de comunicaciones multimedia como Whatsapp o Telegram, generan por sí mismas, y en su relación con millones de smartphones, un nuevo mundo en el que parece que los juristas llegan con retraso, pereza, miedo e ignorancia, a veces (mal) deliberada[2].

Espionaje masivo de smartphones

Pero desde las revelaciones de Edward Snowden[3] sobre el uso y abuso de los metadatos por parte de las agencias de seguridad o servicios de inteligencia como la National Security

---

[2] Sobre el concepto y la jurisprudencia de la ignorancia deliberada, citando la STS Sala de lo Penal de 9 de junio de 2015 (rec. 1665/2014) ver http://www.miguelgallardo.es/ignorancia-deliberada.pdf

[3] Edward Snowden - Wikipedia, la enciclopedia libre
https://es.wikipedia.org/wiki/**Edward_Snowden**
Edward *Joseph* ***Snowden*** *(Elizabeth City, 21 de junio de 1983) es un consultor tecnológico estadounidense, informante, antiguo empleado de la CIA (Agencia Central de Inteligencia) y de la NSA (Agencia de Seguridad Nacional). En junio de 2013, Snowden hizo públicos, a través de los periódicos The Guardian y The Washington Post, documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore*

Agency NSA, el derecho no ha reaccionado ante el espionaje masivo del que todos los usuarios de smartphones son víctimas, lo sepan o no. En España, la Audiencia Nacional se negó a enjuiciar[4] los hechos revelados por Snowden y no constan resoluciones judiciales relevantes sobre el espionaje masivo de la NSA en ningún país del mundo. Tampoco abrió expediente[5] la Agencia Española de Protección de Datos AEPD ni se conoce que otras autoridades garantes de la privacidad nacionales ni europeas como el Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE de la Unión Europea[6] ni el tribunal de europeo de Derechos Humanos[7] lo hayan hecho, al menos eficazmente, hasta ahora.

Más allá de la normativa y la jurisprudencia europea, se ha debatido en las Naciones Unidas sobre el derecho a la intimidad como un grave problema de la humanidad actualmente. El artículo 12 de la Declaración Universal de los Derechos Humanos, dice: "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*". Algunas revelaciones de Edward Snowden señalaban a las mismas Naciones Unidas y a sus más altos representantes como objeto y objetivo del espionaje de la NSA. No solamente fue una cuestión de principios, sino una reacción al espionaje de cargos y funcionarios la resolución A/RES/68/167 "El derecho a la privacidad en la era digital"[8] es pura filosofía moral y política internacionalista que, después de afirmar, reafirmar, observar, acoger, reconocer, destacar, poner de relieve[9] (verbos mucho más filosóficos que los que se emplean en los códigos civiles, administrativos sancionadores o penales), ¿concreta la actuación de la ONU sobre el espionaje masivo?

HABEAS SMARTPHONE y sus habeas metadata/data/audio/video

Aunque no debe confundirse el derecho con el enjuiciamiento para fijar ideas y concretar los paradigmas documentables de la problemática jurídica y pericial de los smartphones, pueden referenciarse algunos casos controvertidos que no sirven de precedente ni de jurisprudencia válida, porque, vistas en perspectiva histórica las resoluciones judiciales, de la misma manera que el derecho informático de los años 80 no producía autos y sentencias sostenibles pocos años después, muy probablemente las primeras resoluciones sobre smartphones tampoco estén creando doctrina científica y jurídicamente sostenible[10].

---

[4] La asociación APEDANICA presentó la querella que puede verse en http://www.miguelgallardo.es/querella-nsa.pdf
agotando los recursos de reforma y apelación. Los documentos judiciales relevantes constan como anexos A2. de la tesis doctoral de Miguel Gallardo en http://miguelgallardo.es/tesis.pdf

[5] La denuncia http://www.miguelgallardo.es/aepd-booz.pdf se presentó contra la empresa Booz Allen Hamilton en la que trabajaba Edward Snowden, siendo particularmente relevante el recurso de reposición contra la resolución de archivo en http://www.miguelgallardo.es/recurso-booz.pdf

[6] Data Protection Directive (95/46/EC) - EUR-Lex - Europa.eu en castellano en http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_es.pdf y en todos los idiomas europeos en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012

[7] Hay al menos dos referencias en el Tribunal Europeo de Derechos Humanos
Application no. 24960/15 en http://hudoc.echr.coe.int/eng?i=001-159526
y Application no. 58170/13 en http://hudoc.echr.coe.int/eng?i=001-140713

[8] Organización de las Naciones Unidas http://www.un.org/es/comun/docs/?symbol=A/RES/68/167

[9] Pág. 69 y ss. o.c. http://miguelgallardo.es/tesis.pdf

[10] En agosto de 2016 la palabra "smartphone" es citada en 67 resoluciones de la jurisprudencia del Consejo General del Poder Judicial en http://www.poderjudicial.es/search/indexAN.jsp

Así las cosas, ha de proponerse alguna definición, aunque sea provisionalmente, para el derecho de los smartphones, diferenciando las teorizaciones especulativas, de las cuestiones y dilemas que afrontan jueces, fiscales y abogados cuando un smartphone es mencionado, o si ni siquiera se menciona pero afecta a hechos relevantes y derechos en un procedimiento judicial. De este derecho del smartphone, un elemento conceptual es el "habeas", en el sentido latino de "tener presente", a semejanza de lo que se expresa en latín casi universalmente con el "habeas corpus", especialmente cuando el juez tiene presente que existe un smarphone y que las acciones u omisiones judiciales pueden afectar a derechos fundamentales de la persona, los colectivos, las sociedades e industrias e incluso a la soberanía de las naciones y al orden económico mundial.

No se trata aquí de detallar todas las tecnologías intrusivas, ni siquiera las que pueden afectar a un teléfono en cualquier país. Deliberadamente se obvian las intervenciones telefónicas clásicas en sistemas equivalentes al SITEL en España, aunque la inmensa mayoría de las escuchas de las que se tiene conocimiento en sedes judiciales dependan de grandes sistemas centralizados que afectan por igual a teléfonos fijos y móviles o celulares, y en estos últimos, incluso con geoposicionamiento retrospectivo bien referenciado[11]. Pero no es una cuestión menor el acceso masivo a todo lo intervenido por orden judicial para el rastreo de indicios mediante inteligencia artificial sobre reconocimiento de voces[12].

La categorización fenomenológica de lo que aquí denominamos "HABEAS SMARTPHONE" [13] debe diferenciar hechos y riesgos, internos y externos, propios y ajenos, legales e ilegales. Pero reiterando que el derecho penal contemporáneo, en la práctica, encuentra sus límites en el enjuiciamiento de lo que puede llegar a ser probado. Los supuestos y las especulaciones teóricas pronto se alejan de la realidad judicial, en la que cada vez son más los smartphones incautados que pasan años sin ser analizados, se tiene conocimiento de impunes intervenciones intrusivas extremadamente perversas y unas pocas personas jurídicas, especialmente un grupo de multinacionales que compiten y cooperan para repartirse un mercado en el que también tratan de protegerse de los intentos de los gobiernos de controlar a quienes controlan a quienes controlan o "metacontrolar".

Desde el robo casual y fortuito de un smartphone que resulta tener datos, audio o vídeo de sensibilidad y riesgo para su propietario pero también para terceros, por ejemplo, si se trata de un abogado cuyos clientes han confiado sus secretos representados en whatsapps o conversaciones o imágenes recuperables, hasta las más excepcionales leyes aplicadas por servicios de inteligencia como la National Security Agency NSA y la Central Intelligence Agency CIA en la lucha contra el terrorismo y el crimen organizado internacional, existe una

---

[11] Sobre SITEL en España http://cita.es/escuchas y documento www.cita.es/sitel.pdf

[12] La misteriosa empresa española AGNITIO se dedica a ello. Pueden encontrarse 184 referencias en los archivos de HackingTeam, 21 en Global Intelligence Files y 6 en The Spy Files según consta en https://search.wikileaks.org/?q=agnitio

[13] La frase legal que aquí se propone se utilizaría en latín, cuya traducción más literal es «tener el smartphone presente» siendo «hábeās» la segunda persona singular del presente de subjuntivo del verbo latino «habēre» (en este caso entendido como «tener»). Es clara la analogía con el "HABEAS DATA" que entre otras fuentes, se trata en https://es.wikipedia.org/wiki/Habeas_data

compleja problemática cambiante y probablemente irrepetible, como el río en el que Heráclito filosofaba que nadie puede bañarse dos veces, porque nunca es el mismo.

En efecto, es inimaginable que se repita alguna vez un caso como el que toda España conoce por el apodo, mote o sobrenombre de su primer protagonista, el "pequeño Nicolás" en cuyas diligencias procesales[14] constan, al menos, tres incidentes muy relevantes y diferenciables para cuanto aquí se entiende y propone como "habeas smartphone". Probablemente existan otras muchas perversiones de smartphones en procedimientos judiciales, pero la variedad y el enredo policial del caso "pequeño Nicolás" es difícilmente igualable, ni siquiera asemejable, al de ningún otro conocido en España hasta ahora.

El primero es el clonado de un iPhone 5 sin orden judicial, utilizando la policía el sistema israelí Cellebrite[15] mediante el cual se vuelca a disco duro y luego a DVDs que constan en el juzgado todo cuanto pudo extraerse del teléfono del detenido, pero sin orden judicial alguna. El clonado de móviles a detenidos en comisarías sin orden judicial motivó una actuación de la Defensora del Pueblo[16] que concluyó recomendando al Ministerio del Interior que el teléfono móvil de los detenidos no fuera clonado sin orden judicial.

El segundo es el uso de antenas falsas de telefonía para vigilar, monitorizar e intervenir el teléfono del Pequeño Nicolás pero también toda la celda delimitada por las estaciones base de la red celular afectando a todo el vecindario de la casa de su abuela (en zona residencial militar y probablemente afectando a cientos de usuarios de telefonía) sin orden judicial[17]. El uso de antenas falsas para la intervención policial masiva de teléfonos smartphones en toda una celda es un problema ya "reconocido", o para mayor precisión, ya se ha conseguido documentar[18] en EEUU mediante la Ley de Libertad de Información (Freedom of Information Act) y se ha planteado como problemática mundial abierta para las Naciones Unidas[19].

El tercero es el uso ilegal de aplicaciones espía o software troyano malware nada menos que en el iPhone 5 del entonces Comisario de Asuntos Internos del Cuerpo Nacional de Policía CNP, Marcelino Martín-Blas, cuyas conversaciones con miembros del Centro

---

[14] Juzgado de Instrucción 2 de Madrid, Diligencias Previas 4676/14 inicialmente contra Francisco Nicolás Gómez Iglesias, pero sobre la que se han abierto piezas separadas que afectan al Comisario de Asuntos Internos y a buena parte de la cúpula policial y Ministerio del Interior de España.

[15] Para información y referencias de los productos para clonado y análisis de smartphones puede verse http://www.cita.es/cellebrite

[16] http://www.cita.es/defensora-del-pueblo

[17] Véase la querella por el uso de antena falsa (IMSI catcher o StingRay) que ni se ha admitido ni tampoco inadmitido, ignorándose pasado más de año y medio en http://www.cita.es/querella-ai ampliada en http://www.cita.es/ampliando-ai y reiterada en http://www.cita.es/reitera-ai

[18] The New York Times "*New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*" by JOSEPH GOLDSTEIN FEB. 11, 2016 http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=0

[19] El escrito dirigido al Dr. Zeid Ra'ad Al Hussein Alto Comisionado de Naciones Unidas para los Derechos Humanos (ACNUDH) en carta abierta por hiperenlaces relevantes en www.cita.es/zeid y www.miguelgallardo.es/zeid.pdf curiosamente acabó en los archivos de HackingTeam publicados por Wikileaks en https://wikileaks.org/hackingteam/emails/emailid/279187

Nacional de Inteligencia CNI fueron intervenidas y grabadas ilegalmente[20]. El Centro Criptológico Nacional CCN del CNI emitió informes supuestamente periciales pero nada concluyentes ni útiles para probar la intrusión a efectos judiciales. Lo más extraño y sospechoso es que el mismo modelo de Apple iPhone ha sido y sigue siendo utilizado por altos cargos y funcionarios públicos, así como por diputados, y nada garantiza que la misma intrusión mediante malware no pueda seguir utilizándose y nadie haya exigido las más básicas responsabilidades, al menos informativas, a la empresa Apple en España[21].

Las aplicaciones (apps) para espiar smartphones forman parte de una perversa industria que se esconde en paraísos fiscales. Cualquiera puede comprar, o para mayor precisión, obtener ilimitadas licencias de programas para espiar smartphones como **FLEXISPY - Spy Phone - Mobile Spy o MSPY** y otros que, ni siquiera cuando se ha evidenciado su uso, la investigación judicial avanza eficazmente. No hay ni una sola referencia a ninguno de esos programas en la jurisprudencia española mínimamente relevante hasta ahora[22].

Las "spy apps" publicitadas hacen la más descarada apología del delito de descubrimiento y revelación de secretos en los ámbitos más íntimos. Parece como si la más mínima sospecha de infidelidad legitimase para intervenir el smartphone de la pareja, y que cualquier indicio de deslealtad laboral permitiera a cualquier patrón espiar a todos sus empleados, impunemente. Desde el 20 de abril de 2016 está pendiente de resolución una doble denuncia[23], por audiovisuales y datos espiados sistemáticamente con sofisticados productos como los mencionados **FLEXISPY - Spy Phone - Mobile Spy - MSPY** ante la Federal Communications Commissions FCC de Estados Unidos y también ante varias autoridades para la privacidad de países europeos, sin constancia de actuación alguna.

Los riesgos, daños y perjuicios relacionados con los smartphones en los procedimientos judiciales no se limitan a las acciones o resoluciones del juez, porque también tiene ua enorme responsabilidad el secretario judicial SJ, que ahora ha cambiado el nombre en España para llamarse letrados de la Administración de Justicia LAJ, como fedatario judicial funcionario público garante de la integridad y autenticidad de todos los documentos, cualquiera que sea su formato. El smartphone no deja de ser un documento en sí mismo, por muy complejo o hipercomplejo que pueda resultar, y es el SJ - LAJ quien debe garantizar no solamente que se investiga eficazmente lo que se debe investigar y que nadie accede a ningún dato, metadato, audio o vídeo sin legitimación y autorización para ello, sino también la disponibilidad de un auténtico medio de vida, pero también un elemento esencial

---

[20] Por esas grabaciones a agentes secretos el juzgado abrió la pieza separada en la que el fiscal puso de manifiesto la gravedad de los hechos y las dificultades para su investigación en un informe que se comenta y se publica íntegro en http://www.cita.es/juzgado-iphone.pdf

[21] Véase el escrito dirigido a APPLE MARKETING IBERIA SAy APPLE RETAIL SPAIN SL Atn.Luis Jonathan Ortiz Finnemore en http://www.cita.es/espionaje-iphone.pdf

[22] Lo que sí existe es una lentísima actuación del JUZGADO DE INSTRUCCIÓN 11 DE MADRID en las Diligencias previas 3034/2013 por descubrimiento de secretos que denunció la ex concejal NOELIA MARTINEZ ESPINOSA contra el actual diputado autonómico y senador JOSE CARMELO CEPEDA GARCIA (que no consta que haya sido citado ni como investigado) sobre las que hay datos y referencias en http://www.cita.es/flexispy-providencia.pdf y http://www.cita.es/querella-flexispy

[23] FCC tickets (#905143) y (#905169) en www.cita.es/fcc-complaint y también en formato PDF con firma criptográfica certificada en http://www.miguelgallardo.es/fcc-complaint.pdf

para la defensa de un creciente número de investigados actualmente en los juzgados de todo el mundo, e incluso antes, cuando son detenidos sin conocimiento judicial alguno.

En este sentido, resulta particularmente indignante que un juez requise docenas de teléfonos smartphones, tabletas, ordenadores personales y sistemas informáticos empresariales, en todo caso, de propiedad privada, y que pasen muchos meses, y en ocasiones varios años, sin que sean devueltos a sus propietarios, más aún cuando son investigados como se pretende llamar ahora en España a imputados, denunciados o querellados en cualquier fase de la instrucción judicial. En definitiva, es preocupante que los juzgados de instrucción acumulen smartphones y otros sistemas durante demasiado tiempo dejando en indefensión a quien necesita sus propios datos y metadatos en el medio de comunicación que es de su propiedad. Es probable que la jurisprudencia solamente avance por autos y sentencias que anulen procedimientos en los que no se ha respetado el derecho que puede derivarse del "habeas smartphone", simplemente, porque no se le ha devuelto a su propietario. En algún caso los abogados se han quejado cada vez más duramente, y en otros, es el smartphone de un abogado investigado el que puede crear problemáticas judiciales extremas[24]. Eso no significa que los smartphones de los abogados merezcan, por sí mismos, una especial consideración, sino que es la condición de abogado de un afectado, y precisamente por ese afectado, por lo que merecen especial protección. La criminalidad de los abogados es compleja y difícil de investigar, pero sus privilegios no pueden impedir la instrucción judicial. Si un abogado, además de ser abogado, es narcotraficante o defraudador, o comete cualquier otro delito que no afecte a la defensa de un cliente concreto, no puede ampararse en su condición de abogado para protegerse, por lo que el "habeas smartphone" de un abogado no debería proteger al abogado en sí mismo, sino solamente a los derechos de sus defendidos respecto a los datos que pudieran obtenerse de su smartphone. En esos conflictivos casos, el necesario "expurgo judicial" es fundamental, porque no todas las partes de un procedimiento tienen por qué tener acceso a todas las evidencias electrónicas que se encuentren en un smartphone. Lo que sí es cierto es que el propietario sí, y pronto, pero el resto, muy limitadamente, no inmediatamente, y siempre tras un responsable y prudente "expurgo judicial" de sus contenidos.

El abogado ejerciente no solamente tiene los límites que marca el Código Penal. Tiene también obligaciones deontológicas o morales más allá de sus propios perjuicios o riesgos. Si un abogado no puede garantizar la seguridad de las comunicaciones con su cliente, o al menos, que si se han espiado no se investiga eficazmente ese espionaje, los derechos fundamentales de todos sin excepción corren serio peligro, especialmente el derecho fundamental de no verse obligado a hacer declaraciones autoinculpatorias y derecho al silencio relacionado con el privilegiado derecho al secreto de las comunicaciones entre

[24] Claros ejemplos de todo ello puede encontrarse en la llamada Operación Púnica cuyos autos 85/2014 del JUZGADO CENTRAL DE INSTRUCCION 6 de la Audiencia Nacional evidencian que varios investigados llevan más de un año sin poder disponer de sus propios smartphones porque no se han podido clonar pese a disponerse en la Policía Judicial de sistemas como el descrito en **www.cita.es/cellebrite** y **www.miguelgallardo.es/cellebrite.pdf**

abogado y cliente[25] cuya violación puede tener consecuencias tan graves como la condena penal y la inhabilitación del juez[26] que ordene la intervención de esas comunicaciones.

El “habeas smartphone”, así como el ya más aceptado habeas data o el menos conocido habeas audio y habeas video, precisa un nuevo planteamiento garantista, en todos los sistemas judiciales del mundo, porque el smartphone del abogado puede ser intervenido de las maneras más sutiles e indetectables que puedan imaginarse. Pero las mismas garantías merece el smartphone del periodista que debe proteger a sus fuentes.

Numerosos periodistas son objeto de investigaciones policiales, con o sin orden judicial, en las que sus smartphones y registros (metadatos) de llamadas entrantes y salientes entregadas sin autorización ni consentimiento ni siquiera con su conocimiento, señalando así a sus fuentes lo que pone en riesgo el derecho a dar y recibir información veraz[27].

Finalmente, los smartphones en los juzgados son también un claro indicador de ciertas problemáticas mucho más generales. Los peritajes judiciales, siempre discutibles desde el primer momento que una parte, o el mismo juez, se plantean consultar a un experto, hasta la última cita o uso sin cita que se haga de los servicios profesionales, condicionan y en muchos casos limitan o imposibilitan que pueda alcanzarse verdad, justicia y reparación. Pocas veces el Poder Judicial se ha tomado en serio a los peritos, y los jueces dejan en manos de secretarios judiciales ahora LAJs o incluso de los funcionarios meros gestores de los procedimientos la designación, nada menos, que del experto a consultar. El resultado es una historiografía de muy lamentables peritajes judiciales sobre diversos smartphones.

Más allá de cualquier normativa siempre mejorable y actualizable, el imperativo categórico de Kant[28] y la lógica deóntica[29] de los “preferidores” racionales o blochianos[30] pueden ser muy útiles para la Filosofía Moral o Ética del descubrimiento y la revelación de secretos en smarphones, que, con toda seguridad, aportará buenas preguntas pero malas conclusiones.

---

[25] El secreto entre abogado y cliente siempre debe ser absoluto o, al menos, el más garantista posible muy especialmente en materia penal en todos los ordenamientos jurídicos mínimamente garantistas (**SUPREME COURT OF CANADA - 13 Feb. 2015 Docket 35399 Att.y General v. Federation of Law Societies of Canada et al)**
https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14639/index.do

[26] Tribunal Supremo de España STS 79/2012, de 9 de febrero de 2012. Sentencia del caso 'Peláez, Crespo y Correa vs. Garzón' por prevaricación judicial con violación de las garantías constitucionales publicada con comentarios sobre la condena del ex juez Baltasar Garzón en http://www.poderjudicial.es/cgpj/es/Poder_Judicial/Tribunal_Supremo/Noticias_Judiciales/Tribunal_Supremo__Sentencia_del_caso__Pelaez__Crespo_y_Correa_vs__Garzon__por_prevaricacion_judicial_con_violacion_de_las_garantias_constitucionales

[27] APEDANICA se ha preocupado por varios incidentes que afectan a la seguridad de periodistas y sus fuentes en gravísimos casos de corrupción que afectan al Poder Judicial y Ministerio del Interior desde una perspectiva internacional. Véanse los escritos dirigidos a la Federación de Periodistas de América Latina y el Caribe FEPALC en www.cita.es/apedanica-fepalc.pdf Reporteros sin Fronteras RSF en www.cita.es/apedanica-rsf.pdf y en inglés a ICIJ en www.cita.es/apedanica-icij.pdf

[28] Sobre el imperativo categórico https://es.wikipedia.org/wiki/Imperativo_categ%C3%B3rico

[29] Deontic Logic G. H. von Wright Mind, New Series, Vol. 60, No. 237. (Jan., 1951), pp. 1-15. en http://www.wnswz.strony.ug.edu.pl/von%20wright,%20deontic%20logic.pdf

[30] Manuel de Ética, Amelia Valcárcel, pág. 121 "*¿Son morales las leyes del mundo?*" disponible en http://www.ipesad.edu.mx/repositorio1/BG-B05-7.pdf.pdf A Ernst Bloch se le conoce y reconoce como el filósofo de las “utopías concretas”, de las ensoñaciones, de las esperanzas. Falta hacen.

Conclusiones, obviamente muy provisionales y relativas:

1º Se sabe muy poco de lo que realmente ocurre o no ocurre y debiera ocurrir ante/con/en/para/por los smartphones, desde una rigurosa perspectiva jurídica y moral, tanto en sedes judiciales, como en comisarías de Policía o en los ámbitos industriales y tecnológicos o en el laboral y deontológico, o en las efervescentes redes sociales y menos aún en el familiar o personal más íntimo.

2º Con toda seguridad, en pocos años se desarrollará el derecho en toda su creciente complejidad y en ese futuro, se llame como se llame, el concepto de "habeas smartphone" pretende definir, dividir categorizando y argumentar jurídicamente sobre un nuevo escenario social condicionado por un pequeño aparato cada vez más sofisticado que se integra en hipercomplejas redes que mezclan la problemática telefónica con la de Internet, explosivamente en todo el mundo. Probablemente sean autos y sentencias con nulidad de actuaciones las que hagan valer el "habeas smartphone", pero antes, las pericias y los peritos deben proponerse con rigor y seriedad poco frecuentes hasta ahora.

3º Ese derecho no puede ser limitado por el ordenamiento jurídico de un único país, sino que estructuras supranacionales como la Unión Europea UE y la Organización de las Naciones Unidas ONU deben preocuparse y más aún, ocuparse seriamente de lo que ocurre y de lo que va a ocurrir con smartphones y sus hipercomplejas redes. Y hará falta mucha Filosofía para todo ello.

Artículo para enviar antes del 10 de agosto de 2016 a
Diego Mauricio Montoya Vacadíez
Director Revista Derecho Penal Contemporáneo
LEGIS Editores.

remitido por

Dr. e Ing. **Miguel Gallardo**, criptólogo y perito judicial privado en España
y
Avv. **Achille Campagna**, abogado y notario ejerciente en San Marino / Italia
ambos en representación de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (**APEDANICA**) entidad sin ánimo de lucro constituida en España en 1992 con Tel. (+34) 902998352 y E-mail: apedanica.ong@gmail.com

La versión definitiva, una vez publicada por la editorial que nos ha invitado, quedará también disponible en www.cita.es/habeas-smartphone.pdf