74/2013

ESTUDIOS DE PROGRESO

Fundación Alternativas

La investigación del delito en la era digital

Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación

Juan Carlos Ortiz Pradillo

FUNDACIÓN alternativas

Juan Carlos Ortiz Pradillo

Licenciado en Derecho con Premio extraordinario (2001) y Doctor en Derecho por la Universidad de Castilla-La Mancha (2005) con la tesis *Las medidas cautelares en los procesos mercantiles* (publicada en la editorial Iustel, Madrid, 2006).

Ha realizado diversas estancias de investigación en la Universidad de Colonia (Alemania) y Florencia (Italia), así como en el Instituto Max-Planck de Derecho Penal Europeo e Internacional de Friburgo, y ha participado en diversos proyectos nacionales de investigación sobre aspectos relacionados con el Proceso civil y el Proceso Penal. Autor de múltiples artículos doctrinales y de más de una docena de capítulos de libros, ha impartido ponencias en Alemania, Italia, Costa Rica y Chile y ha participado en diversos Cursos de Postgrado y Másters de Derecho Procesal Civil y Penal.

Desde 2005 es profesor de Derecho Procesal en la Universidad de Castilla-la Mancha y también es docente de la Escuela de Práctica Jurídica del Ilustre Colegio de Abogados de Toledo.

Maquetación: Isabel Villegas
ISBN: 978-84-15860-08-2
Depósito legal: M-15754-2013

Índice

Abstract

La utilización de los actuales avances tecnológicos en las tareas de investigación criminal por parte de las fuerzas y cuerpos de seguridad del Estado resulta esencial para la persecución y resolución de los delitos, sobre todo en aquellos en los que las Tecnologías de la Información y la Comunicación (TIC) juegan un papel muy importante, y por lo tanto, dicho empleo representa el presente y el futuro de la actividad policial. Por ello, la legislación procesal española debe ser urgentemente reformada e incorporar esas nuevas medidas tecnológicas de investigación criminal con las debidas garantías. En el presente estudio se analizan los déficits legales actuales y se advierten los desafíos jurídicos que representa el empleo de las nuevas tecnologías en las legítimas labores de investigación penal, a la vez que se exponen sólidos argumentos para instar una urgente y necesaria actualización completa de la legislación procesal en España con el fin de adecuarse a las necesidades de la era digital y permitir el uso de las técnicas modernas de investigación que la informática ofrece, de conformidad con los Derechos Fundamentales y la jurisprudencia del Tribunal Europeo de los Derechos Humanos.

The application of Information Technology in the proceedings of criminal investigation is essential for persecution and solution of those crimes in which IT plays important role. The possibility of using new and sophisticated IT's instruments and programs personifies the present and the future of police and judicial investigation. As a consequence, it seems essential that Spanish procedural legislation needs to be reformed in order to apply in our country those new instruments of electronic vigilance, with all the due guarantees. In this analysis, we set out solid arguments to call upon a deep and urgent necessity in Spain of a complete update of the procedural legislation in order to suit the requirements of the digital age and to allow the use of the modern techniques of investigation that computer science provides, in accordance with the European Convention provisions and the ECHR case-law standards that govern electronic investigations.

Resumen ejecutivo

Hubo un tiempo en que la policía no necesitaba más que un arma de fuego, un bloc de notas o una linterna y sus propios sentidos para llevar a cabo sus cometidos, pero desde entonces, al igual que la delincuencia ha aumentado exponencialmente, las técnicas policiales no han parado de evolucionar de forma paralela al propio desarrollo de la humanidad y en la actualidad se valen del manejo de sofisticados instrumentos electrónicos y programas informáticos para todo tipo de actividades, pues la tecnología les brinda la capacidad de amplificar abrumadoramente las capacidades de los agentes policiales en sus tareas de aprehensión, análisis e investigación.

En el anverso de la moneda de este desarrollo tecnológico se encuentran los Derechos Fundamentales de las personas, que necesariamente deben ser reinterpretados para ofrecer una protección adecuada en la nueva Era Digital. ¿Acaso no deberíamos replantearnos la inviolabilidad domiciliaria cuando la mayor parte de nuestra información digital no se halla en los armarios y cajones de nuestras viviendas, sino en Servidores ubicados a millares de kilómetros?, ¿De verdad podemos equiparar la injerencia sobre la intimidad que significa el registro de un equipo informático como si se tratara de la inspección de "papeles y documentos"? En efecto, la utilización de equipos de audio e imágenes térmicas que nos permiten ver y escuchar lo que sucede intramuros de los domicilios es algo más que "poner la oreja" y puede restringir el concepto actual de la inviolabilidad domiciliaria. La posibilidad de escanear los cuerpos de los transeúntes para descubrir si portan explosivos debajo de su ropa o sustancias prohibidas en el interior de su organismo, también excede de lo que constituiría un cacheo policial y exige una reflexión acerca del debate sobre el derecho a la intimidad corporal. Incluso se ha cuestionado si la colocación de una pulsera electrónica de localización para controlar el cumplimiento de las órdenes de alejamiento pudiera afectar a la intimidad de una persona, al convertirse en una especie de sambenito moderno que pudiera desvelar datos de la vida privada de una persona, como es su imputación o condena en un proceso penal.

Con estas premisas, hemos analizado la jurisprudencia de nuestros tribunales respecto al dilema "Tecnología vs. Derechos Fundamentales" y la hemos contrastado con la doctrina de la Corte Suprema norteamericana y del Tribunal Constitucional Federal alemán respecto a la repercusión del desarrollo de la tecnología en el proceso de adaptación de los derechos constitucionales para dar respuesta a los retos planteados por dichos desarrollos.

El hecho de acudir a la interpretación jurisprudencial ha sido consecuencia de otra importante deducción del estudio: desafortunadamente, España se encuentra a la cola de Europa en lo que respecta a la adaptación de la legislación aplicable a la investigación penal a la Era digital y a las nuevas necesidades de protección de los Derechos Fundamentales frente al uso masivo de la tecnología. Tras un profundo estudio jurídico de la legislación y jurisprudencia españolas y su análisis comparativo con lo dispuesto en otros países europeos y en los principales textos de la Unión Europea sobre cooperación en materia penal, hemos comprobado el desfase existente entre la modernidad de los instrumentos tecnológicos aplicables en los operativos policiales frente a la anquilosada legislación procesal al respecto. Mientras la policía española es mundialmente conocida por su conocimiento y uso de técnicas de última generación (balística, dactiloscopia, ciberpatrullaje, etc.) la legislación procesal española sigue anclada en la idea de originales y fotocopias, en la interceptación de telegramas, o en la

inspección "ocular" de la escena del crimen. Contrastan las continuas adaptaciones del Código Penal a las nuevas modalidades delictivas (la última reforma del año 2010 tuvo particular interés en penalizar determinadas actividades delictivas a través de la Red) frente a un sistema procesal penal que sigue hablando de "posaderos y fondistas", "jueces municipales", "jornales de braceros", o multas de "125 pesetas". Más allá de numerosos parches puntuales, ha transcurrido más de una década desde que en el Pacto de Estado de 2001 se acordara la reforma de la vetusta Ley de Enjuiciamiento Criminal, sin la que misma haya visto la luz. Apenas ciertas reformas en el sector de las telecomunicaciones y el comercio electrónico (como la trascendental ley 25/2007 de conservación de determinados datos de las comunicaciones electrónicas) nos permiten a duras penas *salvar los muebles* cuando se trata de investigar la ciberdelincuencia o delitos cometidos gracias a las posibilidades que ofrecen las TIC.

Por todo ello, en el apartado final del presente estudio se formulan interesantes recomendaciones y propuestas de reformas legislativas, a partir de una premisa esencial: la necesidad y urgencia de la reforma de la Ley de Enjuiciamiento Criminal que actualice el régimen jurídico de las medidas de investigación de conformidad con las modernas técnicas que proporcionan los avances tecnológicos, pues a pesar de que el TEDH haya legitimado la jurisprudencia española "complementadora" de la insuficiente regulación legal de las escuchas telefónicas, ha llegado el momento de abordar la necesaria reforma legislativa que permita emplear en nuestro país, con las debidas garantías, los más variados y modernos instrumentos de vigilancia electrónica, sobre todo frente a aquellos delitos en los que la informática y las TIC juegan un papel muy importante. Como bien anticipó el magistrado Ruiz Vadillo en 1988, y hoy sigue siendo suscrito por la principal doctrina española, "las innovaciones tecnológicas -el cine, el video, la cinta magnetofónica, los ordenadores electrónicos, etc.- pueden y deben incorporarse al acervo jurídico procesal en la medida en que son expresiones de una realidad social que el derecho no puede desconocer".

1

Investigación penal en la era de la información

El calificativo comúnmente utilizado para designar la etapa actual en que vivimos es el de la "Sociedad de la información y el conocimiento", vista como la sucesora de la sociedad industrial o postmoderna y caracterizada por el trascendental papel que juegan las tecnologías de la información y la comunicación (en adelante, TIC) en las actividades sociales, culturales y económicas. No obstante, en este trabajo utilizaremos de modo genérico la expresión «Era Digital» para tratar de aunar en dicho término todo lo que ha significado la revolución informática para el desarrollo de la Sociedad de la información y el conocimiento, con particular interés en la transformación que para nuestras vidas ha supuesto la omnipresencia de Internet, debido a que la utilización de múltiples dispositivos electrónicos (teléfonos móviles, *smartphones*, agendas electrónicas, *tablets*, ordenadores portátiles, videoconsolas, etc.) se ha convertido en una parte casi indispensable en nuestro quehacer diario, bien para fines laborales, educativos, trámites administrativos y legales, pero sobre todo, para nuestro tiempo de ocio y para nuestras relaciones sociales.

Si a dicho desarrollo tecnológico le sumamos la reducción de costes en la fabricación y venta de todo tipo de dispositivos electrónicos, es fácil comprobar la universalización del empleo de la informática por cualquier ciudadano, en cualquier parte del mundo y en todos los ámbitos de nuestras vidas, lo cual ha dado lugar a una nueva forma de relación entre el ser humano y las máquinas a través del acopio e intercambio de *bytes* para cualquier actividad: un nuevo comportamiento basado en el "consumo tecnológico" generador de un verdadero *entorno digital* del individuo, que estaría compuesto por toda la información en forma electrónica que, voluntaria o involuntariamente, de forma consciente o inconsciente, el hombre genera con su actividad, no importa dónde se encuentren los archivos informáticos que la contengan o los canales de comunicación a través de los cuales discurra[1].

Cada vez que realizamos o recibimos una llamada telefónica, compramos unos billetes de viaje electrónicos, revelamos a través de Internet las fotos de las pasadas vacaciones, accedemos a un foro o una red social, nos inscribimos a un boletín informativo electrónico o nos descargamos algún archivo en nuestro ordenador, etc., estamos generando una abundante información digital. Basta con *googlearse*[2] para comprobar la

[1] GONZÁLEZ-CUÉLLAR SERRANO, N.: "Garantías constitucionales en la persecución penal en el entorno digital", en VV.AA., *Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García*, ed. Colex, Madrid, 2006, p. 1.

[2] Utilizar los grandes motores de búsqueda de Internet para saber qué se dice de nosotros. Como ejemplo, el motor de búsqueda de Google fue capaz de encontrar, en menos de 0,32 segundos, aproximadamente 94.700 resultados en la Red con el término "Juan Carlos Ortiz Pradillo" (consulta realizada el 22 de abril de 2013).

inimaginable información actualmente disponible en la Red sobre nosotros mismos, y si a dicha información fácilmente accesible a través de la Red le añadimos toda la información sobre nosotros que se encuentra almacenada en las bases de datos de entidades privadas, organismos públicos, etc., el resultado es ciertamente incalculable.

1.1 El uso policial de la tecnología en la investigación penal.

Toda investigación criminal tiene por principal objetivo la obtención de la máxima información posible sobre la comisión de un hecho delictivo (qué sucedió, quiénes intervinieron, cuándo y dónde se produjo) por lo que, debido a esa omnipresencia de Internet en nuestras vidas, así como a la cotidianeidad en la utilización de múltiples dispositivos electrónicos, las autoridades encargadas de la investigación criminal han demostrado un enorme interés en poder acceder y analizar toda esa abundante información digital que diariamente manejamos y utilizarla para la investigación de toda clase de delitos.

La importancia de aumentar la capacidad de las autoridades de utilizar cualesquiera medidas tecnológicas de investigación destinadas a obtener esa información en formato digital se antoja un pilar esencial en cualquier investigación criminal en la actual sociedad informatizada en la que vivimos. De hecho, la principal ventaja del empleo de estas nuevas medidas tecnológicas de investigación reside en su operatividad (transversalidad) para la obtención de evidencias de cualquier clase de delito, sea o no de los denominados "delitos informáticos", pues resultan una eficaz herramienta en la investigación de cualquier tipología delictiva en la que tales dispositivos electrónicos constituyan una valiosa fuente de prueba, debido a sus actuales capacidades de almacenamiento de información y a su empleo para todo tipo de comunicaciones. Por ejemplo, pensemos en las células terroristas que se comunican mediante mensajes en clave o encriptados y publicados en *blogs*; el sicario que porta en su agenda electrónica un listado de sus clientes o de sus futuras víctimas; o el cabecilla de un grupo criminal organizado que guarda en su ordenador portátil documentos electrónicos sobre la contabilidad de sus operaciones, fechas y lugares de recepción y entrega de la mercancía, y los datos de contacto con otras bandas criminales. Ninguno de ellos lleva a cabo delitos informáticos propiamente dichos, pero crean datos digitales que informan del hecho punible[3]. De igual modo, la actual moda juvenil consistente en grabar con un teléfono móvil todo tipo de fechorías (conducción temeraria, vejaciones a compañeros de clase, espiar los probadores femeninos de ropa, etc.) y después "colgarlas" en Internet o a través de las redes sociales son la mejor muestra de cómo la obtención de esa información en formato digital puede ayudar enormemente a la policía en la investigación y resolución de delitos que no son en absoluto delitos informáticos o cibernéticos.

Es más, debido al auge de las nuevas tecnologías de la información y las comunicaciones, la Dirección General de la Policía ha adaptado su estructura interna para responder mejor a los nuevos retos de la criminalidad, entre los que destaca la lucha contra el cibercrimen y la innovación tecnológica a través de la creación de la Unidad de Investigación Tecnológica (UIT), que asumirá la investigación y persecución

[3] GONZÁLEZ-CUÉLLAR SERRANO, N., "Garantías constitucionales…", op. cit., p. 889.

de los delitos a través de las tecnologías de la información y comunicación y actuará como Centro de Prevención y Respuesta del E-Crime de la Policía Nacional[4].

Ahora bien, el uso de la tecnología en las legítimas tareas de investigación por parte de las fuerzas y cuerpos de seguridad del Estado no es en absoluto algo novedoso, sino el resultado de una continua evolución paralela al propio desarrollo de la humanidad. Al igual que la revolución industrial y el desarrollo tecnológico han permitido al ser humano vivir más años, o viajar más rápido y más lejos, también han permitido a las autoridades policiales resolver los delitos de forma más rápida, eficaz y segura. Hubo un tiempo en que la policía no necesitaba más que un arma de fuego, unas esposas, un bloc de notas, y sus propios sentidos para llevar a cabo sus cometidos, y dicha época dio paso al manejo de prismáticos para ver más lejos, micrófonos para escuchar más alto, o perros rastreadores que ayudaran a los agentes en la detección de determinadas sustancias que escapan del alcance del olfato humano. De la misma manera que hemos pasado de viajar a caballo o en carruaje a utilizar modernas aeronaves que nos permiten alcanzar la órbita exterior terrestre, la policía ha pasado de utilizar linternas y prismáticos a manejar modernas herramientas informáticas y dispositivos electrónicos, tanto en el campo analítico forense (dactiloscopia, balística, etc., en donde resulta especialmente destacable el manejo de la Informática forense[5]), así como en el campo operativo, a través de lo que se ha venido a denominar la «vigilancia electrónica[6]».

El ciberpatrullaje y la búsqueda en la Red, el rastreo de ficheros que contengan imágenes y videos de carácter pedófilo, el uso de programas informáticos para la lectura automática de matrículas, la videovigilancia mediante cámaras IP con activación remota, los sistemas de imágenes aéreas, térmicas, de visión nocturna o por satélite, los equipos de reconocimiento biométrico de los rostros de las personas, sus iris, o de bultos sospechosos, o los programas de reconocimiento forense de voces, la utilización de radiobalizas de seguimiento de vehículos, embarcaciones o aeronaves, la utilización de georradares para escrutar y sondear el subsuelo, el empleo de pulseras electrónicas de localización permanente, el uso de la tecnología GPS para conocer la ubicación geográfica exacta de un concreto dispositivo, los sistemas informáticos de detección de tiroteos gracias a la triangulación geográfica del sonido que recogen unos sensores acústicos[7], o el control en tiempo real de los movimientos bancarios y el uso de las

[4] Vid. el Real Decreto 400/2012, de 17 de febrero, que desarrolla la estructura orgánica del Ministerio del Interior.

[5] Ciencia denominada *Computer Forensics*. Como documento clave en materia de legislación, métodos y protocolos y garantías de esta técnica en los EE.UU, véase el manual *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section Criminal Division, September 2009 (http://www.cybercrime.gov). En la doctrina, vid. MACK, M., "Electronic Discovery vs. Computer Forensics", *New Jersey Law Journal*. Vol. 20, October 2003, pp. 1 y ss.; CASEY, E., *Digital Evidence and Computer Crime*, 2nd Edition, ed. Elsevier, London, 2004; KERR, O. "Digital Evidence and the new Criminal Procedure", *Columbia Law Review*, vol. 105, January 2005, pp. 279 y ss., y "Search and Seizure in a Digital World", *Harvard Law Review*, vol. 119, 2006 (http://ssrn.com/abstract=697542).

[6] LLAMAS FERNÁNDEZ, M. / GORDILLO LUQUE, J. M.: "Medios técnicos de vigilancia", en VV.AA.: *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 236. La doctrina norteamericana utiliza los términos "electronic surveillance", "Internet surveillance" y "online surveillance". Vid. BELLIA, P.: "The future of internet surveillance", *The George Washington Law Review,* August, 2004, 72, p. 1375 y ss.; FREIWALD, S.: "Online Surveillance: Remembering the Lessons of the Wiretap Act", *Alabama Law Review*, Fall, 2004, 56, p. 9 y ss.

[7] Sobre el funcionamiento de este sistema, vid. http://www.shotspotter.com/.

tarjetas de crédito, son sólo algunos ejemplos de lo que la tecnología puede facilitar las labores policiales de seguimiento e investigación.

1.2 Las recomendaciones internacionales de incorporar la tecnología a la investigación penal.

Como sabemos, la delincuencia ha sabido adaptarse rápidamente al ciberespacio y a los avances tecnológicos hasta el punto de que una de las principales preocupaciones de los principales organismos internacionales (ONU, la Unión Europea, etc.) es el auge de la utilización de las TIC con fines delictivos. De hecho, los ataques y el espionaje informático se han convertido en la principal preocupación de las distintas agencias de inteligencia y de seguridad de los Estados Unidos, sustituyendo por primera vez al terrorismo internacional en la lista de amenazas del país[8].

Se calcula que más de un millón de personas de todo el mundo son víctimas diarias de la ciberdelincuencia; cada 14 segundos un adulto es víctima de un ciberdelito; y el montante anual de las pérdidas sufridas por actos de ciberdelincuencia ascienden a más de 388.000 millones de dólares (USD), lo que hace que el cibercrimen sea más rentable que el comercio global conjunto de marihuana, cocaína y heroína[9]. Otras estadísticas son aún más alarmantes: en el estudio global de Microsoft sobre ciberacoso, realizado entre febrero de 2011 y enero de 2012 y en el que participaron más de 7.600 niños de 25 países, un 54%, están preocupados por el ciberacoso por Internet, y lo que es más preocupante, el 37% de los jóvenes que navegan por internet han sufrido ciberacoso, y además el 19% de los encuestados afirmó que había ciberacosado a alguien, e incluso un 46% había acosado fuera de Internet a otros jóvenes.

Por tales motivos, las principales instituciones internacionales han recomendado encarecidamente a los Estados la necesidad de adaptar las medidas de investigación recogidas en la legislación procesal penal a la naturaleza específica de las investigaciones referidas a los sistemas informáticos y a las comunicaciones electrónicas, así como profundizar en el ámbito de la asistencia mutua internacional en aquellos casos en los que están involucradas las TIC. Junto con la decisión del grupo *G-8* de crear en 1997 un Subcomité encargado de estudiar los delitos informáticos (*High-tech Crimes*), gracias al cual se han presentado diversos informes y decálogos al respecto, los principales impulsores de aproximar las legislaciones nacionales para adaptarlas a los nuevos retos que plantea el entorno digital han sido el Consejo de Europa y la Unión Europea, cuyas principales propuestas se recogen, de una parte, en la inicial Comunicación *Hacia una política general de lucha contra la ciberdelincuencia*[10], que marcó el objetivo concreto de fomentar la cooperación internacional global en materia de lucha contra la ciberdelincuencia, y más recientemente en el *Plan de Estocolmo*[11], en el que la Unión Europea ha retomado la

[8] Noticia publicada en EL PAÍS el 13 de marzo de 2013. http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html.

[9] Datos extraídos del estudio *The Symantec Internet Security Threat Report 2011* (the Norton Cybercrime Report). http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

[10] Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007. COM (2007) 267 final.

[11] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 20 de abril de 2010, titulado *Garantizar el espacio de libertad,*

tarea de impulsar importantes medidas a adoptar frente a la ciberdelincuencia, y ha dado lugar a la creación del Centro Europeo de Ciberdelincuencia (EC3) en la Oficina Europea de Policía, Europol, en La Haya.

1.3 Contrapartidas del uso de la tecnología ante los tribunales: El "Efecto CSI"

La generalización del uso de la prueba electrónica ante los tribunales presenta, sin embargo, una importante contrapartida a tener en cuenta: las expectativas de contar con una prueba inculpatoria directa de tipo digital que demuestre la comisión del delito de modo que, a falta de una prueba científica, surjan dudas sobre la autoría de los hechos. A medida que se fabrican y emplean nuevos instrumentos y métodos capaces de demostrar científicamente la producción de un hecho, su autor o sus consecuencias, puede llegar a generarse en el juzgador la expectativa de que siempre existirá una prueba científica o electrónica que demuestre el relato de la acusación, pues nos hemos acostumbrado a ver en la televisión grabaciones de videos de seguridad que han filmado la perpetración de un atraco en una sucursal bancaria, una cuchillada en mitad de una riña tumultuaria en un vagón del metro, o una agresión machista en el hall de un hotel. Parece como si en la Era Digital en la que vivimos, siempre debiera existir una evidencia electrónica o científicamente constatable de la comisión de un hecho.

En los EE.UU., en los últimos años se ha alertado frente a los riegos que ha provocado la emisión de determinadas series de televisión cuya temática versa sobre la realización de pruebas científicas forenses en el campo de la investigación criminal, tales como *CSI* o *Bones*, al constatar que los miembros del Jurado tienden a absolver a los acusados en aquellos casos en los que durante el juicio no se presentó una evidencia científica, salvo que se presentara el testimonio de la víctima. Según diversos estudios[12], más de un millar de miembros de Jurados fueron entrevistados antes de su participación como tales en un proceso judicial e interrogados acerca de sus expectativas en cuanto al empleo de pruebas científicas, así como sus hábitos a la hora de ver la televisión y si veían frecuentemente dichas series. Resultó que más de un 46% de los entrevistados esperaba ver alguna prueba científica en todos los casos penales; un 22% esperaba ver pruebas de ADN; un 36 % esperaba ver pruebas de huellas dactilares; y un 32% esperaba ver pruebas del laboratorio balístico de armas de fuego. Clasificados los procesos según el delito enjuiciado, resultó que en los delitos de secuestro y asesinato, un 73% de los miembros de Jurados esperaban ver pruebas de ADN; en los delitos de allanamiento de morada y robo, un 71% esperaba ver huellas digitales; y en los delitos en los que se había utilizado un arma, un 66% esperaba que se expusieran tales evidencias científicas.

Es lo que se ha calificado como el «efecto *C.S.I.*», al atribuir la responsabilidad de tales expectativas a la popular serie de televisión y su progenie, pues los citados estudios arrojaron como resultado que los espectadores de dichas series de televisión tenían

seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo. COM (2010) 171 final.

[12] SHELTON, D.E., KIM, Y.S., BARAK, G., "A Study of Juror Expectations and Demands Concerning Scientific Evidence: Does the 'CSI Effect' Exist?," *Vanderbilt Journal of Entertainment and Technology Law*, 2006, vol. 9, nº2, pp. 331–368; SHELTON, D. E., "The 'CSI Effect': Does It Really Exist?", *NIJ Journal*, Issue No. 259, 2008, pp. 1-7.

mayores expectativas de que se aportaran al juicio pruebas científicas que los miembros del Jurado que no eran espectadores de aquéllas.

Por lo tanto, el empleo de la tecnología en la averiguación de los delitos y la determinación de sus responsables no es simplemente una opción a barajar. Constituye una necesidad en la investigación de determinados delitos, principalmente en aquellos en los que se emplean las nuevas tecnologías —ciberdelincuencia—, pero también puede llegar a constituir una fuerte expectativa por aquellos que están llamados a valorar la veracidad de las pruebas presentadas y su fuerza inculpatoria, sobre todo cuando se trata de juicios ante el Tribunal del Jurado, a la hora de contrarrestar la presunción de inocencia del acusado.

2

Investigación criminal tecnológica y fronteras nacionales

2.1 La deslocalización de la información digital

El primer gran desafío al que se enfrenta la persecución penal en la Era Digital radica en la deslocalización de la información digital a conseguir, ya que la misma puede ser «accesible» desde nuestros hogares sin necesidad de estar «localizada» dentro de los confines de nuestro domicilio.

Como sabemos, una de las principales diligencias judiciales de investigación que se ordena cada vez más frecuentemente consiste en ordenar la clonación y el examen forense de los discos duros y elementos periféricos de los equipos informáticos aprehendidos tras un registro domiciliario, así como de cualquier otro dispositivo electrónico de comunicación o almacenamiento. Sin embargo, al movernos en un *entorno digital* e interconectado a nivel mundial, la óptica desde la que enfocar esas tareas de incautación de la información digital debe ser sustancialmente distinta al tradicional enfoque con el que se procede a un registro domiciliario en el mundo corpóreo, pues la protección constitucional y legal del domicilio es claramente insuficiente para la salvaguardia del *entorno digital*[13], pues está claro que el contenido vendría constituido por la información digital, con independencia del tamaño o formato utilizado, pero el continente no tiene por qué ser el equipo informático a través del cual dicha información fue creada, recopilada, transformada o emitida. Dicho equipo puede ser simplemente un medio a través del cual la información digital fue colocada en otro lugar, otro *continente*[14]. En estos casos, ¿puede accederse legítimamente a la información que no está almacenada físicamente en el equipo investigado, sino en otra parte del mundo, pero sí resulta accesible a través de dicho equipo?

Es preciso tener en cuenta, además, que esta deslocalización de la información almacenada se hace cada vez más habitual en aquellos entornos que trabajan conforme a lo que se conoce como "técnicas de computación en la nube (*Cloud Computing*)", en donde la información se almacena de manera permanente en servidores alojados en cualquier parte del mundo y se envía, a través del acceso a Internet, a cachés temporales del ordenador de sobremesa del cliente, su portátil, PDA, etc. La importancia de atajar con prontitud los problemas legales y jurisdiccionales derivados del uso de la computación en nube es vital si tenemos en cuenta que se calcula que actualmente un 7% del contenido digital está en la nube y se prevé que en 2016 será el 36%[15].

La trascendencia jurídica de la ubicación física de las pruebas electrónicas, a los efectos de lograr su incautación cuando se encuentran en el extranjero, nos hace recordar que la expresión "Internet no conoce fronteras" favorece al delincuente, porque en el plano policial las fronteras nacionales se convierten en auténticos obstáculos para las legítimas

[13] GONZÁLEZ-CUÉLLAR SERRANO, N.: "Garantías constitucionales…", op. cit., p. 891.
[14] Entiéndase por «continente» tanto el habitáculo o recipiente, como "cada una de las grandes extensiones de tierra separadas por los océanos", según define la RAE el término "continente".
[15] http://econsultancy.com/uk/blog/10469-this-week-s-top-six-infographics-16.

labores de investigación y recogida de las evidencias de dichos delitos. Las fuerzas y cuerpos de seguridad deben respetar la soberanía de otros países y, como norma general, no pueden llevar a cabo actividades de investigación y obtención de pruebas fuera de su jurisdicción[16]. Se hace preciso una inmediata colaboración internacional, que no siempre llega a tiempo, bien porque el país requerido no disponga de la tecnología adecuada para cumplir con la orden solicitada, bien porque el tiempo que transcurra hasta su realización no impida que las pruebas puedan alterarse o destruirse, o bien porque dicho país simplemente no atienda a la ayuda reclamada.

A tales problemas se suma el hecho de que los delitos cometidos a través de las TIC merecen ser calificados como «delitos cometidos a la velocidad de la luz[17]», al ser ejecutados mediante instrumentos electrónicos y cuyas evidencias pueden ser alteradas o destruidas tan rápidamente como son creadas. Surge así la necesidad de impulsar instrumentos jurídicos internacionales que sirvan de referencia, no sólo para la armonización de las conductas criminalizadas por parte de los diferentes Estados, sino también para la regulación de nuevas modalidades de investigación y una rápida cooperación judicial y policial entre las autoridades de los diferentes países de cara a la obtención de las evidencias del delito cometido.

De otra parte, los delitos cometidos a través de Internet serían encuadrables dentro de los denominados «delitos a distancia», los cuales suelen presentar una importante fragmentación geográfica en su desarrollo, y por ello, originan problemas relativos a la determinación del tiempo y lugar su comisión[18]. Esto es, se trata de delitos en los que resulta habitual que entre el lugar desde el que el sujeto lleva a cabo el acto ilícito y el lugar en el que se produce la ofensa al bien jurídico exista una notable distancia geográfica que obliga a determinar la competencia territorial entre los órganos jurisdiccionales.

La falta de armonización en la respuesta penal a los delitos informáticos puede dar lugar a paraísos cibernéticos similares a los refugios de piratas que florecieron en el Caribe en el siglo XVIII: una base de operaciones de refugio para aquellos que generan ingresos por aprovecharse de los extranjeros[19]. Pero existe un riesgo mayor: que la disparidad en torno al régimen de persecución judicial contra los ciberdelincuentes debido a la falta de colaboración de las autoridades nacionales, la diversidad de capacidades técnicas de investigación y capacidades forenses, así como la escasez de personal bien preparado, conviertan al ciberespacio en un *reino de Taifas* similar al surgido en España en el siglo XI tras la desaparición del Califato de Córdoba.

2.2 La obtención transfronteriza de la prueba electrónica

[16] En el mismo sentido, CSONKA; P.: "The Council of Europe´s Convention on Cyber-Crime and other european initiatives", *Revue Internationale de Droit Pénal*, 2006, vol. 77, p. 477. GERCKE, M.: Understanding cybercrime: a Guide for Developing Countries, 2009. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[17] Vid. BRENNER, S., "At light speed: attribution and response to cybercrime/terrorism/Warfare", *Journal of Criminal Law & Criminology,* 2007, nº97, pp. 379 y ss.

[18] GONZÁLEZ TAPIA, M. I., "El concepto de delito a distancia", en *VV.AA. (Coordinador: Juan José GONZÁLEZ RUS), El Código Penal de 1995, cinco años después*, ed. Servicio de Publicaciones de la Universidad de Córdoba, Córdoba, 2002, p. 101.

[19] Vid. BRENNER, S. W. / SCHWERHA IV, J. J., "Cybercrime Havens. Challenges and Solutions", *Business Law Today*, vol. 17, nov-dec. 2008, pág. 50.

Para evitar tales inconvenientes, la principal solución pasa por aumentar la cooperación judicial internacional para luchar contra esta nueva amenaza global. Y así, cada vez son más los instrumentos supranacionales que prevén la intervención de las autoridades encargadas de la investigación criminal más allá de sus fronteras territoriales, tal y como sucede, por ejemplo, con la Decisión Marco sobre equipos conjuntos de investigación[20], el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea[21], el Convenio del Consejo de Europa sobre el Cibercrimen[22], o más específicamente, la Propuesta de Directiva sobre el Exhorto Europeo de Investigación Penal[23], con el fin de facilitar la cooperación judicial en la obtención de pruebas en procesos penales transfronterizos.

La posibilidad de tomar conocimiento de lo que sucede más allá de nuestras fronteras sin necesidad de "poner un pie" en territorio extranjero no es nada novedoso, pues no hay que olvidar que ya en la antigüedad se construían torres de vigilancia para conocer lo que sucedía más allá de las tierras del reino, o que en la I Guerra Mundial se utilizaban globos aerostáticos con fines igualmente observatorios. Pero resulta que la posibilidad de aprehender información digital que se encuentre localizada más allá de las fronteras nacionales también ha sido perfeccionada. Los denominados "registros transfronterizos de equipos informáticos" (*Cross-Border Searchs*) ya se encuentran expresamente previstos, tanto en determinadas leyes domésticas, como en ciertos tratados y textos internacionales.

A nivel internacional, su uso legal ya fue propuesto en la Recomendación R (95) 13 del Consejo de Europa[24], de tal modo que las autoridades pudieran extender el registro de equipos informáticos a esos otros sistemas que se hallaran conectados al equipo originariamente investigado y apropiarse de los datos almacenados en aquéllos, incluso si tales sistemas informáticos se encontraran en una jurisdicción extranjera[25]. En segundo lugar, la Unión Europea también era partidaria de admitir los registros transfronterizos en determinados casos excepcionales o de urgencia, como por ejemplo, *para impedir la destrucción o alteración de pruebas de un delito grave o para impedir la comisión de un delito del que pueda seguirse con probabilidad la muerte o una lesión física grave de una persona (...) y a efectos de investigación de un delito penal*

[20] Decisión Marco 2002/465/JAI del Consejo, de 13 de junio de 2002, sobre equipos conjuntos de investigación (DOUE L 162, de 20 de junio de 2002). Vid. también el art. 8 de la Ley 11/2003, de 21 de mayo, reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea (BOE núm. 122, de 22 de mayo de 2003).

[21] Convenio de 29 de mayo de 2000 (DOCE C 197, de 12 de julio de 2000).

[22] Convenio del Consejo de Europa firmado en Budapest el 23 de noviembre de 2001, y en vigor en España desde el 1 de octubre de 2010. Véase el Instrumento de Ratificación del Convenio (BOE de 17 de septiembre de 2010). El listado de países que han ratificado dicho Convenio puede consultarse en: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=14/02/2012&CL=ENG.

[23] Propuesta de Directiva del Consejo y del Parlamento Europeo relativa al exhorto europeo de investigación penal (DOUE C 165, de 24 de junio de 2010).

[24] Recomendación R (95) 13, del Comité de ministros del Consejo de Europa, de 11 de septiembre de 1995, relativa a los problemas de la legislación procesal penal conectados a las tecnologías de la información.

[25] *The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required.*

grave[26]. El Convenio sobre el Cibercrimen recogió finalmente tal posibilidad, aunque con importantes límites, pues el art. 32 autoriza los accesos transfronterizos a datos almacenados, pero sólo cuando se trate de *datos informáticos almacenados de libre acceso al público (fuentes abiertas) o con el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático*[27].

Por ello, en ausencia de un régimen internacional adecuado, no faltan voces que defienden la unilateralidad a la hora de proteger los intereses nacionales frente a ataques provenientes del extranjero[28], y muchos países han procedido a incorporar dentro del catálogo de medidas legales de investigación criminal ciertas medidas de alcance extraterritorial, como son los registros transfronterizos de equipos informáticos.

Como ejemplos, Australia permite extender el examen del equipo informático con motivo de un registro domiciliario, tanto a los datos contenidos en cualquier dispositivo de almacenamiento de datos extraíble, como a los datos almacenados en un dispositivo en una red informática de la que el equipo investigado forme parte[29], incluidos los datos no almacenados en el domicilio (*including data not held at the premises*), y si dicho registro se prevé que tenga efectos extraterritoriales, la *Surveillance Devices Act* de 2004 dispone que el juez comunique dicha medida de investigación a la autoridad competente de dicho país extranjero, entendiendo por dicha autoridad quien pudiera conceder, conforme a las leyes de dicho país, similares medidas de vigilancia. En los EE.UU., se ha admitido jurisprudencialmente la admisibilidad de los registros transfronterizos para la obtención de datos almacenados en un equipo, aunque éste se encuentre en un país extranjero, y su validez probatoria en el posterior proceso judicial en territorio norteamericano[30]. En Holanda también cabe extender el registro de un equipo informático conectado a la red a otros sistemas que se encuentren conectados al equipo originariamente investigado, siempre que dichos sistemas sean legalmente accesibles a la persona que habitualmente utiliza o trabaja con dicho equipo, aunque en

[26] Posición Común 1999/364/JAI, de 27 de mayo de 1999, relativa a las negociaciones del proyecto de Convenio sobre el Cibercrimen (DOUE L 142, de 5 de junio de 1999. Vid. art. 1, apartado 7).

[27] El primer caso se refiere, por ej., a los supuestos en que se trata de información disponible en páginas web a las que se puede acceder sin una clave (vid. GERCKE, M.: *Understanding cybercrime*…, op. cit., p. 207), mientras que el "consentimiento voluntario de persona autorizada" sólo permite a las autoridades solicitar dicho consentimiento pero no ordenarlo, a diferencia de lo regulado en el art. 18 (orden de comunicación). Vid. el apartado 293 del Informe explicativo del Convenio: *they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article*.

[28] GOLDSMITH, J. L., "Cybercrime and Jurisdiction". Presentation at the *Conference on International Cooperation to Combat Cyber Crime and Terrorism,* Hoover Institution, Stanford University, Stanford, California, Dec. 6-7, 1999.

[29] Subsección 3C y siguientes de la Crimes Act de 1914, modificada en virtud de la Cybercrime Act 2001 (Ley nº161/2001).

[30] El caso más conocido fue *United States v. Gorshkov* [2001 WL 1024026 (W.D. Wash. 2001)], en el que agentes del FBI obtuvieron pruebas alojadas en un equipo informático en Rusia. Como estudio en el que se analizan los casos más destacados y los principios que sustentarían estas medidas unilaterales, vid. GOLDSCHMITH, J.: "The Internet and the Legitimacy of Remote Cross-Border Searches", *Public Law and Legal Theory Working Paper no. 16*, 2001. A favor de tales medidas, vid. SEITZ, N.: "Transborder Search: A New Perspective in Law Enforcement", *Yale Law School 2004*, (*http://www.yjolt.org/files/seitz-7-YJOLT-23.pdf*); BRENNER, S. / KOOPS, B. J.: "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law*, 2004, Vol. IV No. 1, pp. 1 y ss.; ADLER, A.: "The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act", *University of Miami Law Review,* January, 2007, vol. 61, pp. 393 y ss., y BELLIA, P. L., "Chasing Bits across Borders", *The University of Chicago Legal Forum*, 2001, pp. 35-101.

la praxis se ha entendido tales registros no pueden exceder de las fronteras holandesas en coherencia con los principios del Derecho internacional[31]. Lo mismo se prevé en Bélgica, si bien para el supuesto de que dicha búsqueda implique un registro transfronterizo, se establece la posibilidad de copiar esos datos localizados en un Estado extranjero, en cuyo caso, el juez de instrucción debe informar inmediatamente al Ministerio de Justicia, "quien informará en su caso a las autoridades competentes del Estado interesado, si se puede determinar razonablemente[32]". Y en Portugal, la Ley portuguesa sobre el Cibercrimen[33] posibilita extender el registro de un equipo informático a aquellos otros sistemas que resulten accesibles a través del equipo inicialmente examinado, cuando existan motivos suficientes para creer que los datos solicitados se encuentren en aquéllos, con expresa mención a los correos electrónicos y demás comunicaciones electrónicas, requiriéndose siempre autorización judicial, y aplicándose en todo lo no previsto la normativa establecida para la intervención de la correspondencia.

La conclusión es evidente. España debería, no sólo regular expresamente el examen y registro de equipos y dispositivos informáticos, sino también la posibilidad de extender tales registros a otros sistemas que se encuentren conectados al equipo originariamente investigado, cuando existan indicios de localizar en esos otros sistemas información relevante para la causa.

3

[31] Art. 125j del Código Procesal Penal. Vid. DE HERT, P., "Cybercrime and Jurisdiction in Belgium and the Netherlands", en KOOPS, B .J. / BRENNER, S. W., Cybercrime and Jurisdiction. A Global Survey, ed. T.C.M. Asser Press, 2006, The Hague, p. 108.

[32] Art. 88ter del Código Procesal Penal, reformado en el año 2000 a través de la *Loi du 28 novembre 2000 relative a` la criminalite´ informatique*.

[33] Ley nº 109/2009, de 15 de septiembre, por la que se aprueba la ley del cibercrimen, se transpone al ordenamiento jurídico interno la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero, sobre los ataques contra los sistemas de información, así como se adapta la ley al Convenio del Consejo de Europa sobre el Cibercrimen (publicada en el Diario de la República, serie 1ª, núm. 179, de 15 de septiembre de 2009).

Investigación criminal tecnológica y derechos fundamentales

Tal y como hemos constatado, el uso policial de la tecnología para la investigación y resolución de los delitos es el resultado de una continua evolución ligada al propio desarrollo de la humanidad. Por ello, de igual modo que los avances tecnológicos se emplean en la telemedicina o en la ingeniería biomédica, pueden y deben ser utilizados por las autoridades policiales para resolver los delitos de forma más rápida, eficaz y segura. Al fin y al cabo, la utilización de la tecnología por parte de las fuerzas y cuerpos de seguridad no significa otra cosa que amplificar de forma abrumadora sus sentidos, su pericia y sus métodos de actuación.

No obstante, no podemos pasar por alto la incidencia que el desarrollo de las TIC puede llegar a tener en la posible afectación a los Derechos Fundamentales, de modo que se hace necesario analizar los desafíos éticos y jurídicos que los desarrollos relativos a las nuevas tecnologías pueden suscitar en el proceso de adaptación de los derechos constitucionales para dar respuesta a los retos planteados por dichos desarrollos[34].

En efecto, la utilización de equipos de audio e imágenes térmicas que nos permiten ver y escuchar lo que sucede intramuros de los domicilios es algo más que "poner la oreja" y puede restringir el concepto actual de la inviolabilidad domiciliaria. La posibilidad de escanear los cuerpos de los transeúntes para descubrir si portan explosivos debajo de su ropa o sustancias prohibidas en el interior de su organismo, e incluso de llegar a prevenir conductas sospechosas gracias a programas informáticos de análisis de la conducta humana, también excede de lo que constituiría un cacheo policial para descubrir las pertenencias que la persona lleve encima y exige una reflexión acerca del debate sobre el derecho a la intimidad corporal. El cotejo de los datos de posicionamiento GPS de un terminal de telefonía móvil para conocer en tiempo real los desplazamientos o la posición geográfica de un determinado ciudadano excede de lo que pudiera constituir un seguimiento policial. Incluso se ha cuestionado si la colocación de una pulsera electrónica de localización para controlar el cumplimiento de las órdenes de alejamiento pudiera afectar a la intimidad de una persona, al convertirse en una especie de sambenito moderno que pudiera desvelar datos de la vida privada de una persona, como es su imputación o condena en un proceso penal[35].

Tales avances son vistos con enorme recelo por cierto sector doctrinal, pero también por los propios tribunales, preocupados principalmente por la insuficiencia de la regulación legal en lo que respecta al empleo de instrumentos tecnológicos en la investigación criminal y su posible afectación desproporcionada a la intimidad y a otros derechos fundamentales de los sujetos pasivos de las investigaciones. Por ello, a continuación se

[34] DÍAZ REVORIO, F. J., "La constitución ante los avances científicos y tecnológicos: breves reflexiones al hilo de los recientes desarrollos en materia genética y en tecnologías de la información y la comunicación", *Revista de Derecho Político de la UNED*, nº 71-72, 2008, pp. 87-110.
[35] NIEVA FENOLL, J., "Las pulseras telemáticas: aplicación de las nuevas tecnologías a las medidas cautelares y a la ejecución en el proceso penal", *Revista del poder judicial*, núm. 77, 2005, p. 209.

expondrán las tesis manejadas por varios tribunales constitucionales a la hora de validar o no el empleo de medidas tecnológicas de investigación penal.

3.1 La doctrina del Tribunal Supremos de EE.UU. ante el debate entre intimidad y tecnología

Un interesante ejemplo de ponderación judicial sobre la proporcionalidad de los nuevos instrumentos tecnológicos y su empleo en las labores de investigación criminal, a la hora de determinar si vulneran o no los derechos fundamentales de las personas, lo constituye la doctrina de la Corte Suprema estadounidense relativa a la Cuarta enmienda (protección de la intimidad frente a pesquisas y registros) y a la necesidad de que las autoridades policiales necesiten de una orden judicial previa para poder llevar a cabo determinadas actuaciones que puedan considerarse "búsquedas y registros" a efectos constitucionales.

Hasta los años 60, dicha doctrina fundamentaba la protección de la privacidad en la idea de la propiedad. Ejemplo de ello lo constituye el caso *Olmstead*[36] (1928), en donde la Corte Suprema estimó que la grabación policial de las conversaciones telefónicas no vulneraba la protección constitucional de la Cuarta Enmienda porque no se había llevado a cabo una "invasión física de su domicilio[37]", mientras que en el caso *Silverman*[38] (1961) declaró que la instalación de un micrófono en la pared exterior adyacente a la vivienda ―instrumento denominado comúnmente "spike mike"― sí constituía un registro ilegal a los efectos de la cuarta enmienda, porque constituía una entrada física en las propiedades de los acusados.

Fue tras la sentencia del caso *Katz*[39] (1967) cuando la Corte Suprema estadounidense proyectó la protección constitucional sobre las comunicaciones telefónicas en atención a la "expectativa razonable de privacidad del individuo" en relación con la Cuarta Enmienda, superando la doctrina restrictiva basada en la afectación a la propiedad que había sido emitida anteriormente y declarando que la Constitución "protege personas, no lugares", y advirtiendo que la aplicación de la Cuarta Enmienda depende de si la persona que invoca su protección puede reclamar dicha expectativa legítima en atención a dos criterios: de un lado, si la persona ha mostrado una real (subjetiva) expectativa de privacidad, y de otro lado, si los poderes públicos deben reconocer dicha expectativa como "razonable". Así, por ejemplo, en el caso *Smith v. Maryland*[40] (1979), el Tribunal Supremo validó la instalación de un "pen register" en las oficinas centrales de una compañía telefónica para grabar los números marcados por el sujeto investigado desde el teléfono de su domicilio, al considerar que los ciudadanos no tienen una expectativa razonable de privacidad sobre los números marcados.

A partir de entonces, la Corte Suprema ha manejado tres elementos principales con el fin de responder a la pregunta de si un actor estatal ha superado los límites de la Cuarta Enmienda en los casos en los que se empleen "nuevas tecnologías" en la investigación

[36] Olmstead v. United States, 277 U.S. 438 (1928).
[37] Ídem, párrafo 466.
[38] *Silverman v. United States*, 365 U.S. 505 (1961).
[39] *Katz v. United States*, 389 U.S. 347 (1967).
[40] *Smith v. Maryland*, 442 U.S. 735 (1979).

criminal[41]. En primer lugar, ¿cuál es el objetivo de la vigilancia a través de instrumentos tecnológicos? es evidente que la vivienda de una persona recibe una mayor protección que la propiedad comercial, pues el domicilio es el lugar elegido por excelencia por las personas para desarrollar su vida privada. En segundo lugar, ¿qué clase de información se revela con dicho tipo de vigilancia? Allí donde la vigilancia técnica revele detalles íntimos o privados es más probable que se considere que alguno de los derechos de privacidad de la cuarta enmienda ha podido quedar vulnerado, pues no es lo mismo grabar los movimientos de una persona por las calles de una ciudad, que en el interior de un gimnasio. Y en tercer lugar, y éste es un dato muy importante, ¿cuál es la naturaleza de los medios técnicos utilizados? La Corte Suprema norteamericana ha estimado que la utilización de instrumentos tecnológicos de investigación que son ampliamente utilizados y conocidos por los ciudadanos conducen a una menor expectativa de privacidad que los que son menos conocidos o no están, en general, a disposición del público. Es decir, la Corte Suprema ha tenido en cuenta la naturaleza y grado de desarrollo de la tecnología aplicada a la investigación en sí misma con el fin de determinar si la expectativa razonable de un individuo a la privacidad ha sido violada o no, y exigir una orden judicial previa habilitadora de las actuaciones policiales investigadoras.

Por ejemplo, en el caso *Ciraolo*[42] (1986) se llegó a la conclusión de que la utilización de un helicóptero y una cámara fotográfica de 35 mm para fotografiar una plantación de marihuana en una finca no constituía una violación de la Cuarta Enmienda, ya que la droga podía ser apreciada a simple vista, que el uso de helicópteros y avionetas privadas se ha convertido en una práctica cotidiana a nivel comercial, y que la protección de la Cuarta Enmienda de la casa nunca se ha ampliado para exigir a la policía cerrar sus ojos al caminar por la calle o, como en el caso examinado, al sobrevolar una casa, pues dicha vigilancia en helicóptero se llevó a cabo de forma visual sin el empleo de complejos instrumentos tecnológicos. Por el contrario, en el caso *Dow Chemical*[43] (1986), la Corte Suprema declaró que la vigilancia de la propiedad privada mediante el uso de equipos de vigilancia por satélite, de carácter muy complejo y que no están generalmente disponibles al público, podría ser constitucionalmente proscrita en ausencia de una orden judicial. Y de igual modo, en *Kyllo*[44] (2001), el debate giró en torno al grado de intromisión de los instrumentos y equipos de investigación utilizados, en un caso en donde se utilizaron dispositivos de visión térmica para percibir desde la vía pública las emanaciones térmicas producidas dentro de un domicilio donde se sospechaba que se estaba cultivando marihuana con lámparas de rayos UVA. El tribunal sentenció que la información revelada por tales dispositivos "no sería posible sin la intrusión física en una zona protegida por la Constitución y que la misma se había obtenido con el empleo de tecnología que no está en uso público en general".

En el caso *Knotts*[45] (1983), se legitimó la instalación de un radiotransmisor en una lata de cloroformo que la policía vendió al sospechoso y que éste dejó en el interior de su vehículo, al reconocerse la validez del seguimiento policial de dicho vehículo por las

[41] JACOBY, N., "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States", *Georgia Journal of International and Comparative Law*, vol. 35, 2007, nº3, pág. 453.
[42] *California v. Ciraolo*, 476 U.S. 207 (1986)
[43] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986)
[44] *Kyllo v. United States*, 533 U.S. 27, 34 (2001).
[45] *United States v. Knotts*, 460 U.S. 276 (1983).

carreteras y vías públicas, tras estimar la Corte Suprema que una persona que viaja en un automóvil en la vía pública no tiene ninguna expectativa razonable de privacidad en sus movimientos de un lugar a otro, y consideró equiparable dicho seguimiento a la vigilancia visual, pues "nada de lo dispuesto en la Cuarta Enmienda prohíbe a la policía de aumentar las facultades sensoriales otorgadas desde el nacimiento con las mejoras que les brinda la ciencia y la tecnología". Por el contrario, en el asunto *Karo*[46] (1984), se estimó que la utilización de un radiotransmisor para conocer los movimientos de un sujeto dentro de su residencia privada requería una decisión judicial previa (warrant), por no constituir un "lugar abierto a la vigilancia visual" y reconocer que "las residencias privadas son lugares en los que el individuo normalmente espera una intimidad libre de injerencias gubernamentales no autorizadas por una orden judicial". A todo ello hay que sumar lo resuelto en el caso *Jones*[47] (2012), en donde la Corte Suprema ha valorado, no sólo el desarrollo de la tecnología y del instrumento utilizado, sino también el grado cuantitativo de la injerencia sobre la privacidad de los individuos. Si en el caso *Knotts* el dispositivo de seguimiento se empleó durante unas horas, en el caso *Jones* la policía controló los movimientos del vehículo del sospechoso las 24 horas del día durante 28 días, y éste es uno de los motivos por los cuales el Alto Tribunal llega a la conclusión de que "el seguimiento GPS durante un largo plazo en las investigaciones de la mayoría de los delitos afecta a las expectativas de privacidad".

Por último, y aunque aún no ha llegado ningún caso a la Corte Suprema, varios tribunales inferiores han estimado que la persona que instala en su ordenador un programa P2P que habilita para compartir archivos, dando así a cualquier persona con acceso a Internet la posibilidad de acceder a su equipo para descargarse dichos archivos, no tiene ninguna expectativa razonable de privacidad en los contenidos compartidos de ese equipo, de modo que no vulnera la Cuarta Enmienda la posibilidad de que la policía pueda utilizar un determinado *software* para localizar y descargar de forma remota tales archivos compartidos, incluso aunque el equipo informático en el cual se almacenan los mismos se encuentre en el domicilio del sospechoso[48].

3.2 La doctrina del Tribunal Constitucional alemán con motivo de los avances tecnológicos

Si la Corte Suprema estadounidense ejemplifica a la perfección la ponderación de derechos fundamentales en los sistemas *Common Law*, el Tribunal Constitucional alemán es el espejo donde se miran muchos de los tribunales constitucionales del sistema continental a la hora de interpretar las garantías derivadas de las Constituciones modernas, y es también otro de los órganos jurisdiccionales que más se ha preocupado por la posible afectación a los Derechos Fundamentales originada con motivo de los avances tecnológicos.

Por todos es conocida la sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983[49], relativa a la Ley del Censo de la República Federal Alemana, en la

[46] *United States v. Karo*, 468 U.S. 705 (1984).
[47] *United States v. Jones*, 565 U.S. (2012).
[48] Vid. *United States v. Ladeau*, 2010 WL 1427523 (D. Mass. 2010); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Borowy*, 577 F.2upp.2d 1133, 1136 (D. Nev. 2008); y *United States v. Heckenkamp*, 482 F.3d 1142, 1146-1147 (9th Cir. 2007).
[49] Sentencia de la Primera Sala, del 15 de diciembre de 1983 (1 BvR 209, 269, 362, 420, 440, 484/83).

que se alude al «Derecho a la autodeterminación informativa» como el derecho de los ciudadanos a conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos; un derecho que conlleva la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. Pero el reconocimiento de dicho Derecho Fundamental y la preocupación del protector constitucional germano sobre la afectación a los Derechos Fundamentales "debido a las condiciones actuales y futuras del procesamiento automático de datos" ya se apuntó en el conocido caso del *microcenso*[50] (1969), en donde ya se advertía que sería incompatible con la dignidad humana que el Estado pudiera apelar al derecho de registrar y catalogar en forma coercitiva la totalidad de la personalidad de los seres humanos, incluso en el anonimato de una encuesta estadística.

Otro importante debate constitucional en torno al dualismo intimidad-tecnología se produjo con la regulación de la medida de investigación denominada «vigilancia acústica del domicilio» (*Grosser Lauschangriff*), hasta el punto que motivó la modificación de la Constitución germana en virtud de lo declarado por el Tribunal Constitucional alemán en 2004[51], y en dicha sentencia se aprecia como lo debatido no era tanto la posibilidad del legislador de permitir dicha medida de investigación con el fin constitucionalmente legítimo de perseguir la delincuencia, sino la forma y modo en que debía llevarse a cabo la vigilancia del domicilio particular, pues para el intérprete germano "existe un núcleo inviolable en el que el particular desarrolla su vida privada, el cual debe ser respetado por el Estado al llevar a cabo medidas de vigilancia".

Otra medida tecnológica de investigación analizada por el Tribunal Constitucional alemán fue la utilización de las balizas de seguimiento GPS por parte de la policía, legitimadas en el año 2005[52], en donde se volvió a advertir de los peligros que el desarrollo de la tecnología puede suponer para el derecho a la privacidad. En aquel caso, el tribunal estimó que el uso de la tecnología GPS para revelar la ubicación de una determinada persona o su permanencia en un lugar determinado, aunque significaba una injerencia sobre el derecho a la intimidad del sospechoso, su alcance e intensidad no llegaban a tal nivel que se entendiera vulnerada la dignidad humana o su núcleo de desarrollo de la vida privada, si bien el tribunal constitucional advirtió de la necesidad de estar atentos ante el rápido desarrollo de las tecnologías de la información y su uso como medidas de investigación que pudieran vulnerar el derecho constitucional a la autodeterminación informativa, en el sentido de posibilitar una vigilancia total sobre un sujeto (*Rundumüberwachung*) y construir un perfil integral de la personalidad de un individuo que sería constitucionalmente inadmisible.

Otro ejemplo de ponderación judicial de la posible afectación a los Derechos Fundamentales derivada del desarrollo tecnológico fue el caso referido a los «registros

[50] Sentencia de la Primera Sala, del 16 de julio de 1969 (1 BvR 19/63) sobre la Ley sobre la Realización de una Estadística Representativa de la Población y de la Vida Económicamente Activa (microcenso) de 16 de marzo de 1957 (BGBl I, p. 213), en la versión de la ley de 5 de diciembre de 1960 (BGBl I p. 873).
[51] Véase la Sentencia del Tribunal Constitucional alemán de 30 de marzo de 2004 (1 BvR 2378/98, 1 BvR 1084/99).
[52] Sentencia de 12 de abril de 2005 (2 BvR 581/01). La ponderación realizada por el Tribunal Constitucional germano entre los derechos constitucionales a la intimidad y al libre desarrollo de la personalidad del sospechoso y la proporcionalidad de aquella medida policial de investigación ha sido convalidada posteriormente por el TEDH (S. de 2 de septiembre de 2010, caso *Uzun c. Alemania*).

online» de equipos informáticos (*online Durchsuchung*) del año 2008[53], en donde el Tribunal germano reconoció que "las garantías legales y constitucionales derivadas de los Derechos al secreto de las comunicaciones e inviolabilidad del domicilio, así como las acuñaciones que del Derecho a la Personalidad se habían hecho a través de la jurisprudencia constitucional, no habían tenido suficientemente en cuenta la necesidad de protección de la intimidad frente al desarrollo de las técnicas informáticas, por lo que su cobertura resultaba insuficiente para dicha protección" y consagró un nuevo contenido para el Derecho a la autodeterminación informativa: el Derecho Fundamental a la garantía de la confidencialidad e integridad de los equipos informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*) y estableció férreos requisitos para que dicha medida tecnológica de investigación criminal fuese compatible con las garantías constitucionales.

Y también debe indicarse que, en el año 2010, el intérprete constitucional germano vuelve a advertir el riesgo de que el uso de la tecnología, a través del acopio y cruce masivo de datos, pueda dar lugar a la creación de los referidos "perfiles de personalidad" de los ciudadanos hasta el punto de llegar a influir de manera determinante en el comportamiento de los individuos[54], lo cual entiende que no sólo va en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar. Con motivo de un recurso de inconstitucionalidad contra las reformas que tenían por misión incorporar al Ordenamiento jurídico germano la Directiva 2006/24/CE sobre conservación de datos de las comunicaciones electrónicas, el Tribunal Constitucional alemán declaró en su sentencia de 2 de marzo de 2010[55] que dicha regulación vulneraba dos principios clave: el principio de proporcionalidad (*Verhältnismäßigkeit*) y el principio de determinación jurídica o claridad legal (*Normenklarheit*), pues aunque la efectividad de la persecución criminal, la defensa de la Seguridad y el cumplimiento de las tareas de los servicios de inteligencia son fines legítimos que pueden constituir una injerencia justificada en el secreto de las telecomunicaciones, y aunque tal Derecho Fundamental no prohíbe cualquier almacenamiento de datos de tráfico, la regulación impugnada suponía un almacenamiento desproporcionado "con una extensión como hasta ahora el Ordenamiento no había conocido previamente, pues abarca todo el período de seis meses y prácticamente todos los datos de tráfico de las comunicaciones de todos los ciudadanos sin conexión con una conducta reprochable atribuible, incluso de modo abstracto, a una peligrosidad o una situación cualificada (…). Dependiendo de la utilización de las telecomunicaciones y el futuro de tal aumento de la densidad de almacenamiento, puede permitir la producción significativa de perfiles de personalidad y de movimiento de prácticamente todos los ciudadanos, aumenta el riesgo de los ciudadanos a estar expuestos a mayores y posteriores investigaciones, sin ni siquiera el

[53] BverfG, 1 BvR 370/07, de 27 de febrero de 2008. Como estudio detallado sobre dicha medida, véase mi trabajo "El registro 'online' de equipos informáticos como medida de investigación contra el terrorismo (Online Durchsuchung)", en VV.AA., *Terrorismo y Estado de Derecho*, ed. Iustel, Madrid, 2010. pp. 457-478.

[54] Como hiciera en 1983, el TC germano cita un ejemplo concreto: quien crea que, por ejemplo, la participación en una asamblea o una iniciativa ciudadana será registrada por las autoridades y que ello pueda generarle algún riesgo, posiblemente renunciará al ejercicio de su derecho fundamental reconocido en los arts. 8 y 9 de la Ley Fundamental.

[55] BVerfG, 1 BvR 256/08, que resuelve los procesos BvR 256/08, 263/08 y 586/08.

motivo para el que se ha dado el uso, y evoca un sentimiento de vaga amenaza que puede afectar a un ejercicio imparcial de los derechos fundamentales en muchos ámbitos".

3.3 La postura de los Tribunales Españoles sobre la aplicación de la tecnología a la investigación criminal

Es importante advertir que no existe precepto legal alguno en nuestra legislación procesal que establezca cómo y cuándo poder utilizar un perro adiestrado para localizar la droga que pueda pretender introducirse de forma ilegal en España, o qué maquinaria puede emplearse para rastrear el subsuelo en busca de los cuerpos de unos menores presuntamente asesinados a manos de su progenitor o para ver en la oscuridad qué embarcaciones tratan de alcanzar la costa española, o cuándo utilizar ultrasonidos para detectar falsas paredes y techos que escondan alijos de drogas o armas en el interior de una vivienda, y sin embargo, su utilización resulta cada vez más habitual y no se cuestiona. Por el contrario, tales dudas acerca de su admisibilidad y constitucionalidad sí que se plantean cuando lo que se debate es la utilización de un scanner corporal para localizar la droga u otros objetos que un individuo pueda portar consigo, un dispositivo de localización GPS para controlar los movimientos de un vehículo, o un micrófono para grabar las conversaciones que puedan realizarse en un determinado espacio cerrado.

Los reparos más importantes advertidos por los tribunales españoles en orden a su licitud y su admisibilidad probatoria se deben a la conjunción de la obsoleta legislación procesal junto con la enorme lesividad que el empleo de la tecnología puede generar sobre importantes garantías constitucionales tales como la intimidad, la libertad de expresión, el secreto de las comunicaciones, la inviolabilidad del domicilio, la protección de datos personales o el secreto profesional. Por ello, en España también se ha producido un interesante debate jurisprudencial referido a la aplicación de la tecnología a las medidas de investigación criminal y su posible incidencia en la afectación a determinados Derechos Fundamentales.

3.3.1 La ponderación entre intimidad y tecnología del Tribunal Constitucional español

Existe una dilatada doctrina del Tribunal Constitucional referida a la protección de los Derechos fundamentales, con especial atención al Derecho a la intimidad, frente a los continuos avances tecnológicos, pues el Tribunal Constitucional ha afirmado de forma reiterada que el derecho a la intimidad ha adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, orientada a su plena efectividad, "razón por la que se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, *sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada*" (STC 119/2001, de 29 de mayo).

El mejor exponente de la ponderación realizada por nuestro Tribunal Constitucional entre la protección de los derechos fundamentales de la persona y el empleo de la tecnología, cuando se persigue un fin legítimo como es la investigación criminal por parte de las autoridades judiciales y policiales, lo representa la STC 173/2011, de 7 de

noviembre, en donde expresamente se pronuncia sobre la necesidad de establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas -en particular, la intimidad personal- a causa del uso indebido de la información así como de las TIC durante la investigación criminal.

Al igual que en su momento advirtiera el Tribunal Constitucional alemán, una de las mayores preocupaciones del intérprete español también gira en torno a la posible eliminación de cualquier núcleo de privacidad de los individuos con motivo del acopio y cruce masivo de datos gracias a las posibilidades que ofrece la informática, con el riesgo de crear «perfiles integrales de la personalidad» de los ciudadanos. Por ello, nuestro Tribunal Constitucional considera necesario *establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información,* y dispone que cualquier injerencia en el contenido de un ordenador personal deberá venir legitimada, en principio, por el consentimiento de su titular, o bien por una previa resolución judicial, salvo en los casos en los que se estime necesaria y urgente la actuación policial, porque entiende que "el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.), no sólo forma parte de este mismo ámbito, sino que además, a través de su observación por los demás, pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico (…), está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad, por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona".

3.3.2 La legitimidad del uso de la tecnología en la investigación criminal para el Tribunal Supremos español

El Tribunal Supremo se ha pronunciado reiteradamente sobre la legitimidad de la utilización de las nuevas capacidades tecnológicas por parte de las fuerzas y cuerpos de seguridad del Estado, consciente de que la inexistencia de una normativa expresa que regule la posibilidad de utilizar los nuevos avances tecnológicos supone acrecentar las desventajas con las que se encuentran las fuerzas y cuerpos de seguridad a la hora de proceder a la indagación y descubrimiento de los instrumentos y pruebas de los delitos, y ha defendido el deber de la jurisprudencia de suplir las insuficiencias de la legislación procesal española respecto a determinadas medidas limitativas de derechos fundamentales *hasta que se produzca la necesaria intervención del legislador*[56].

[56] Doctrina sustentada en la STC 49/1999, de 5 de abril, referida a las insuficiencias legales del art. 579 LECrim.

En primer lugar, es posible discernir un importante grupo de sentencias dictadas por el Tribunal Supremo, sobre todo durante el año 2008, en las que se validó el empleo de diversos instrumentos tecnológicos, para lo cual lo examinado fue la naturaleza de la información obtenida y el Derecho fundamental que podría considerarse comprometido. No es lo mismo entender afectado el Derecho Fundamental a la intimidad (apartado 1º del art. 18 CE) que el Derecho al secreto de las comunicaciones (apartado 3º de dicho artículo), pues la injerencia sobre el secreto de las comunicaciones requiere siempre resolución judicial, mientras que «no existe en la Constitución reserva absoluta de previa resolución judicial respecto del derecho a la intimidad personal», de modo que aunque se ha reconocido también respecto del derecho a la intimidad personal, como regla general, la exigencia de monopolio jurisdiccional, se ha admitido de forma excepcional *que en determinados casos y con la suficiente y precisa habilitación legal sea posible que la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas*, siempre que respeten las exigencias dimanantes del principio de proporcionalidad, y existan razones de urgencia y necesidad que motiven la intervención policial inmediata[57].

Junto con esta diferenciación respecto al derecho afectado, el Tribunal Supremo también ha distinguido entre la obtención de «datos de tráfico» referidos a comunicaciones electrónicas y la obtención de «datos de carácter personal», y a partir de dicha diferenciación, el Tribunal Supremo ha legitimado la utilización de un scanner para la captación policial de los códigos IMSI e IMEI correspondientes a los terminales de telefonía móvil[58], el empleo de *software* para la obtención de la dirección IP mediante rastreos policiales en Internet de datos procedentes de programas P2P[59], o el uso de radiotransmisores (balizas de seguimiento GPS) para la localización de embarcaciones en alta mar[60], por estimar que su empleo policial para la localización geográfica de determinados dispositivos electrónicos en absoluto vulnera el derecho fundamental al secreto de las comunicaciones o supone una injerencia excesiva sobre el derecho fundamental a la intimidad, a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional.

Para el Tribunal Supremo, la ausencia de relevancia constitucional se deriva, bien de que se trata de "diligencias de investigación legítimas desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiriera en un derecho fundamental que requeriría la intervención judicial" (en el caso del empleo de balizas GPS), bien de que lo único que hace la policía es obtener una "información de conocimiento público para cualquier usuario de Internet y que el propio usuario de la red es quien lo ha introducido en la misma" (en el caso del rastreo de direcciones IP), bien que se trata de actuaciones equivalentes a "una labor de vigilancia convencional" (en el caso de la captura de los códigos IMSI/IMEI). Por ello, la utilización policial de novedosos instrumentos electrónicos en labores de investigación criminal ha sido admitida con carácter general por nuestro Tribunal Supremo, sin plantearse esa distinción norteamericana respecto a si la tecnología empleada es o no sofisticada o conocida comúnmente por la sociedad.

[57] El TS asume, de este modo, esa diferenciación expuesta por el TC en sus SSTC 70/2002 y 123/2002.
[58] SSTS de 20 de mayo y de 18 de noviembre de 2008, y de 28 de enero de 2009.
[59] SSTS de 9 de mayo y 28 de mayo de 2008.
[60] Vid. SSTS de 22 de junio de 2007, 11 de julio de 2008, y 19 de diciembre de 2008.

De igual modo, también ha legitimado reiteradamente uno de los avances tecnológicos más utilizado en la lucha contra el crimen: el sistema informático SITEL de interceptación de las telecomunicaciones en sustitución de las grabaciones en cintas magnetofónicas. En numerosas sentencias, el Tribunal ha analizado el rango jurídico de la regulación de los requisitos técnicos y operacionales para proceder a ejecutar los mandamientos judiciales de interceptación de las comunicaciones[61], el funcionamiento de los servidores centrales y los niveles de seguridad en cuanto al acceso a la información allí alojada y su grabación en un DVD sellado digitalmente para su posterior entrega a la autoridad judicial[62], el bloqueo de los datos contenidos en el servidor central una vez que concluye la investigación que motivó la interceptación y el régimen de su posterior borrado físico a instancias de la autoridad judicial[63], así como la autenticidad y ausencia de manipulación de tales DVD con los datos volcados del servidor[64], hasta llegar a concluir que el SITEL *cumple con todas las exigencias y garantías propias de esta clase de diligencias de investigación y probatorias que cuentan con una previa autorización judicial para su práctica*[65].

4

[61] STS, sala 3ª, de 5 de febrero de 2008 y STS, sala 1ª, de 20 de mayo de 2008.
[62] SSTS de 13 de marzo, 29 de junio, 6 de julio y 5 de noviembre de 2009.
[63] SSTS de 14 de abril y 6 de junio de 2011.
[64] Especial atención merece la STS de 30 de diciembre de 2009 y los votos particulares a la misma. Sobre dicha sentencia, vid. RODRÍGUEZ LÁINZ, J. L., "De vueltas con SITEL", *La Ley*, núm. 7515, de 23 de noviembre de 2010.
[65] SSTS de 31 de marzo, 12 de abril, y 19 de julio de 2010.

Desafíos de la investigación penal en la era digital: El caso paradigmático del control sobre las telecomunicaciones

Debido a la cotidianeidad en el uso de Internet y de los demás medios de comunicación, una de las diligencias de investigación casi indispensable para la resolución de los delitos suele ser el acceso a las comunicaciones efectuadas por el presunto autor de los hechos (ya sean simplemente telefónicas —llamadas, sms, o datos de geolocalización — como electrónicas —páginas web visitadas, correos electrónicos, mensajes enviados o recibidos a través de programas informáticos, etc.—).

Es entonces cuando surgen importantes dificultades a la hora de admitir nuevas medidas tecnológicas de investigación y nuevas fórmulas de injerencia en el contenido de las comunicaciones cibernéticas, debido a que el actual —e insuficiente— régimen legal de la interceptación de las comunicaciones telefónicas establecido en el art. 579 LECrim es el marco jurídico aplicable a la decisión judicial de interceptar las comunicaciones electrónicas y telemáticas de una persona, y muy particularmente las comunicaciones efectuadas a través de Internet, pues a él se remiten, entre otras, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (en adelante, LGT), así como la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (en adelante, LCDCE).

Desde el 31 de marzo de 2006, en España hay oficialmente más líneas de teléfono móvil que habitantes, y a finales de diciembre de 2011, el número de líneas de telefonía móvil era de unos 56.189.478, frente a 47.157.822 habitantes, siendo la tasa de penetración de 111,5 líneas por cada 100 habitantes[66]. A ello habría que añadir el número de ordenadores portátiles, *tablets* y agendas electrónicas que utilizan tarjetas SIM de telefonía móvil para conectarse a la red, así como videoconsolas, televisores de última generación, etc., aptos para la comunicación a través de Internet y que se utilizan constantemente para acceder a la red y compartir archivos, música o películas, comunicarse a través de las redes sociales, etc. Es más, el impacto de los aparatos telefónicos de última generación (*Smartphones*) en el acceso a Internet a través de la telefonía móvil es tal que los ciberataques se han trasladado también a la telefonía móvil. De acuerdo con el Informe McAfee sobre amenazas correspondiente al cuarto trimestre de 2011[67], casi todas las categorías de *malware* y de *spam* han experimentado descensos en su crecimiento, con excepción del *malware* para móviles, que ha aumentado durante el último año y ha puesto sus ojos en el sistema operativo Android para dispositivos móviles. Durante el segundo trimestre del año 2012, un estudio realizado por la empresa de seguridad Kaspersky identificó un total de 15.000 nuevas muestras de malware contra Android —principalmente, programas troyanos multifuncionales capaces de robar datos de estos dispositivos, además de descargar

[66] Información disponible en la página web de la CMT: http://www.cmt.es/cmt_ptl_ext/SelectOption.do.
[67] Disponible en: http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q4-2011.pdf.

módulos adicionales de servidores gestionados por los atacantes[68]—. Y se prevé que en el futuro aumenten estos ataques contra terminales móviles, sobre todo en lo que se refiere a las operaciones bancarias que se realizan mediante dispositivos móviles, ya que cada vez más ciudadanos gestionan sus finanzas a través de los móviles.

Por ello, la declaración del juez Ruiz Vadillo en el célebre ATS de 18 de junio de 1992 (caso *Naseiro*), de que el régimen del art. 579 LECrim era aplicable, no sólo a la primitiva telefonía por hilos sino también a las modernas formas de interconexión por satélite, ondas, etc., resultó todo un acierto y una premonición en aquel momento[69], pues en la Era Digital actual, tanto la regulación legal como la correspondiente interpretación jurisprudencial de los límites y garantías que rodean al derecho fundamental al secreto de las comunicaciones están llamadas a desempeñar un papel clave en la investigación criminal, y dada la vital importancia que las comunicaciones electrónicas han adquirido en el presente y que aumentará exponencialmente en un futuro próximo, resulta sencillo concluir la magnitud que alcanzará la protección de la intimidad en el sector de las comunicaciones electrónicas.

4.1 La transcendencia del régimen legal de la interceptación de las comunicaciones telefónicas y su jurisprudencia

A pesar de la trascendencia de la necesaria y debida regulación legal de la posibilidad de controlar e interceptar las comunicaciones realizadas a través de medios telemáticos, poco ha cambiado en España desde que se reformara el archiconocido art. 579 LECrim en 1988 para permitir la intervención de las comunicaciones telefónicas como medida de investigación procesal, pues la redacción originaria del art. 579 LECrim hablaba de la "detención, apertura y examen de la correspondencia postal y telegráfica[70]". Pero el dilatado retraso en el tiempo de tal regulación normativa, con entrada en vigor casi diez años después de la promulgación de la Carta Magna, *no se vio compensado, en absoluto, con claridad, precisión y detalle, (...) sino que, antes al contrario, escaso y gravemente deficiente, el referido precepto ha venido precisando de un amplio desarrollo interpretativo por parte de la Jurisprudencia constitucional y, más extensa y detalladamente incluso, por la de esta misma Sala (...), enumerando con la precisión exigible todos y cada uno de los requisitos, constitucionales y de legalidad ordinaria, necesarios para la correcta práctica de estas restricciones al secreto de las comunicaciones*[71].

Como decimos, han transcurrido casi 25 años desde dicha reforma legal, y a pesar de la incesante demanda por parte de los órganos jurisdiccionales de que el legislador proceda a adecuar la legislación procesal al cumplimiento y garantía de los requisitos y límites establecidos por el Tribunal Constitucional, lo cierto es que los cambios más

[68] Informe IT Threat Evolution: Q2 2012, disponible en la página web http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012.

[69] Vid. Posteriormente las SSTS de 8 de febrero de 1999 y de 19 de febrero de 2007: "...el ámbito de protección de este medio de comunicación -la telefonía- no tiene limitaciones derivadas de los diferentes sistemas técnicos o avances tecnológicos del momento que puedan emplearse".

[70] Reformado a través de la Ley Orgánica 4/1988, de 25 de Mayo, de Reforma de la Ley de Enjuiciamiento Criminal en materia de delitos relacionados con la actividad de bandas armadas o de elementos terroristas o rebeldes (BOE núm. 126, de 26 de mayo de 1988).

[71] STS de 19 de septiembre de 2004.

importantes se han producido en el ámbito jurisprudencial, y motivados por la necesidad de cumplir con las sentencias condenatorias dictadas por el TEDH contra España con motivo de dicha diligencia de investigación.

En efecto, la evolución jurisprudencial de las escuchas telefónicas en España podría quedar sintetizada en tres etapas diferentes, que se corresponderían con tres importantísimas resoluciones del TEDH[72]: en primer lugar, la STEDH *Valenzuela Contreras vs. España*, de 30 de abril de 1998 (aunque para unos hechos sucedidos con anterioridad a la reforma legal española de 1988), en donde el Tribunal Europeo declaró que el derecho interno español cumplía con el requisito de la accesibilidad, pero no con el requisito de la previsibilidad en sentido estricto, ya que *«algunas de las condiciones que se desprenden del Convenio, necesarias para asegurar la previsibilidad de la «ley» y garantizar en consecuencia el respeto de la vida privada y de la correspondencia, no están incluidas en el art. 18.3 CE ni en las disposiciones de la LECrim (...), principalmente la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial, la naturaleza de las infracciones a que puedan dar lugar, la fijación de un límite de la duración de la ejecución de la medida, las condiciones de establecimiento de los atestados que consignen las conversaciones interceptadas, y, la utilización y el borrado de las grabaciones realizadas»*. En segundo lugar, y ya referida expresamente a la adecuación del reformado art. 579 LECrim, la STEDH *Prado Bugallo vs. España* de 18 de febrero de 2003, en la que el Tribunal Europeo volvió a dictar una condena contundente contra España por insuficiencia y falta de calidad de la ley española. Y en tercer lugar, el Auto de Inadmisión de 25 de septiembre de 2006 (caso *Abdulkadir Coban vs. España*), en donde el TEDH admitió finalmente la tesis del gobierno español de que el régimen legal para las intervenciones telefónicas se funda, no solamente en los arts. 18.3 CE y 579 LECrim, sino también en las precisiones y condiciones establecidas por la jurisprudencia.

Para el TEDH, las insuficiencias de la ley española de 1988 han sido paliadas por la jurisprudencia, principalmente del Tribunal Supremo y del Tribunal Constitucional a partir del ATS de 18 de junio de 1992, a partir del cual la "previsibilidad" de la ley en sentido amplio no puede ser cuestionada y *contiene reglas claras y detalladas y precisa, a priori, con suficiente claridad y extensión las modalidades de ejercicio del poder de apreciación por las autoridades en el ámbito considerado*, si bien reconoce que *sería deseable una modificación legislativa que incorpore estos principios o garantías jurisprudenciales*[73].

4.2 Nuevos desafíos de la interceptación de las telecomunicaciones en la era digital

[72] MUÑOZ DE MORALES ROMERO, M., "Hacia la cobertura legal de las intervenciones telefónicas en el ordenamiento jurídico español: La reforma del art. 579 LECrim", *Boletín de la Facultad de Derecho de la UNED*, nº 27, 2005, pp. 47-92.

[73] "Bien qu'une modification législative incorporant à la loi les principes dégagés de la jurisprudence de la Cour soit souhaitable, tel que le Tribunal constitutionnel l'a lui-même constamment indiqué, la Cour estime que l'article 579 du code de procédure pénale, tel que modifié par la loi organique 4/1988 du 25 mai 1988 et complété par la jurisprudence du Tribunal suprême et du Tribunal constitutionnel, pose des règles claires et détaillées et précisent, *a priori*, avec suffisamment de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré".

Los avances tecnológicos plantean importantes desafíos jurídicos en cuanto a la investigación y prueba de aquellos delitos que se ejecutan a través de la Red, y en general, de cualquier conducta antijurídica que se sirva de la evolución de la ciencia y la tecnología, bien para la comisión delictiva, bien para evitar su descubrimiento. Sin embargo, y tal como advierte Galán Muñoz, *ni los enormes avances tecnológicos, ni la gran variedad de novedosas técnicas de comunicación existentes en Internet, ni el desarrollo de una importante y compleja normativa destinada a establecer un sistema facilitador de la investigación de los delitos cometidos en el seno de esta red, han provocado cambio alguno en la Ley de Enjuiciamiento Criminal española*[74]. Las conductas delictivas más peligrosas a las que se enfrentan hoy los Estados (terrorismo, la delincuencia organizada transnacional, tráfico de drogas, armas y seres humanos, la explotación sexual de menores y la pornografía infantil, la delincuencia económica y la corrupción, y por supuesto, el cibercrimen) se han adaptado muy rápidamente a los cambios en la ciencia y la tecnología, en su intento de aprovecharse ilegalmente y socavar los valores y la prosperidad de nuestras sociedades abiertas[75]. Y sin embargo, para luchar judicialmente frente a los desafíos derivados de la Sociedad de la Información y la Comunicación del siglo XXI, contamos con una legislación procesal nacida a finales del siglo XIX.

Por todo ello, y a pesar de que el TEDH ha legitimado el actual régimen legal y jurisprudencial aplicable en España a las medidas limitativas del derecho fundamental al secreto de las comunicaciones, consideramos que ha llegado el momento de abordar la necesaria reforma de la legislación procesal española para poder emplear en nuestro país, con las debidas garantías, esos nuevos instrumentos de vigilancia electrónica en las tareas de investigación criminal, con especial atención a aquellos delitos en los que la informática juega un papel muy importante (la delincuencia informática, y muy especialmente, la ciberdelincuencia).

El motivo es claro: España se encuentra en estos momentos a la cola de Europa en lo que respecta a la adaptación de su legislación procesal a este nuevo entorno digital producido con motivo del auge de las TIC, a diferencia de lo acontecido en otros países europeos, que han reformado expresamente su legislación procesal con el objetivo de atajar los nuevos problemas que plantea la delincuencia informática, y han aprovechado para regular nuevas medidas tecnológicas de investigación[76].

---

[74] GALÁN MUÑOZ, A., "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", *Revista Penal*, nº24, julio 2009, p. 100.

[75] Comunicado del Consejo de la Unión Europea *Proyecto de Estrategia de Seguridad Interior de la Unión Europea: "Hacia un modelo europeo de seguridad",* Bruselas, 23 de febrero de 2010. Documento 5842/2/10, JAI 90.

[76] Por ejemplo, Bélgica reformó su legislación procesal penal en el año 2000, a través de la Ley de 28 de noviembre de 2000 relativa a la criminalidad informática, para introducir nuevas medidas tecnológicas de investigación. El Reino Unido también adaptó su legislación en el año 2000 a través de la *Regulation of Investigatory Powers Act* (RIPA). En Francia, destacan la Ley de 5 de enero de 1988 sobre el fraude informático, la Ley de 23 de enero de 2006 sobre la lucha contra el terrorismo y la adopción de medidas diferentes a los controles de seguridad y de frontera, y más en particular, el plan de lucha contra los delitos informáticos de 14 de febrero de 2008. Y en Italia sobresalen el "Codice della privacy" a través del Decreto legislativo núm. 196 de 30 de junio de 2003; el Decreto Ley núm. 144, de 27 de junio de 2005, sobre medidas urgentes de lucha contra el terrorismo internacional; el Decreto de 16 de agosto de 2005 sobre medidas preventivas de adquisición de los datos personales de las personas que usan los lugares públicos de servicios de telecomunicaciones no supervisado o puntos de acceso a Internet

La propuesta de reforma de la LECrim aprobada en el Consejo de Ministros de 22 de julio de 2011, junto con la propuesta de "Ley Orgánica de desarrollo de los derechos fundamentales vinculados al proceso penal", no llegaron a tiempo de ser estudiadas y debatidas en profundidad antes del final de la legislatura, a pesar de que constituían un importante paso hacia delante en el objetivo de actualizar el régimen jurídico de las diligencias de investigación *a las exigencias de las nuevas tecnologías de la información y del entorno digital propio de la sociedad del siglo XXI* (vid. Exposición de Motivos). Más recientemente, el Ministerio de Justicia acaba de dar a conocer el 25 de febrero de 2013 la propuesta de texto articulado de la Ley de Enjuiciamiento Criminal.

Por todo ello, a continuación se pondrán de manifiesto los debates más importantes que se han generado a propósito de la aplicación del art. 579 LECrim tras el desarrollo de las TIC, con el fin de servir de guía al legislador para proceder a reformar nuestra decimonónica LECrim. Tales debates pueden quedar englobados en torno a cuatro ámbitos muy significativos: la legalidad, la judicialidad, la motivación y la proporcionalidad.

4.2.1 El debate sobre la legalidad: modalidades de interceptación no previstas en la ley

La suficiente previsión legal de las medidas limitativas de los derechos fundamentales y las libertades públicas constituye un requisito esencial a la hora de garantizar su constitucionalidad y las exigencias de seguridad jurídica en dicho ámbito, e implica importantes garantías respecto del contenido de la Ley, que debe garantizar "la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho[77]", o dicho con palabras del TEDH, "una norma es previsible cuando está redactada con la suficiente precisión que permite al individuo regular su conducta conforme a ella y predecir las consecuencias de la misma; de modo que la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la claridad suficiente para aportar al individuo una protección adecuada contra la arbitrariedad[78]".

Resulta evidente que la LECrim de 1882, si no pudo contemplar las intervenciones telefónicas, mucho menos aún pudiera atisbar los nuevos avances tecnológicos, y de ahí que, al igual que en su momento se realizó una interpretación amplia de los conceptos penales de «documento» para incluir dentro del mismo la cinta magnetofónica, el disquete, el CD-ROM, etc., o de «moneda» para incluir en el mismo la falsificación de tarjetas de crédito, en estos años se ha defendido una interpretación judicial integradora del art. 579 LECrim para legitimar la intervención de los correos electrónicos y de los demás tipos de comunicaciones realizadas a través de Internet[79], aunque también se ha

mediante tecnología inalámbrica; o la Ley núm. 281, de 20 de noviembre de 2006, sobre las escuchas telefónicas.

[77] STC 36/1991, de 14 de febrero.

[78] Entre otras, vid. SSTEDH *Malone*, de 2 de agosto de 1984; *Piermont*, de 27 de abril de 1995; *Hashman y Harrup*, de 25 de noviembre de 1999; *Amann*, de 16 de febrero de 2000, o *Rotaru*, de 4 de mayo de 2000.

[79] Vid., HERNÁNDEZ GUERRERO / ÁLVAREZ DE LOS RÍOS, "Medios informáticos y proceso penal", *Estudios Jurídicos. Ministerio Fiscal,* 1999-IV, p. 497; GARCÍA RUIZ, J. M., "Correo

propuesto que esas nuevas modalidades, por encontrarse ayunas de regulación procesal penal, exigen una nueva y minuciosa previsión legislativa[80].

La cuestión es: ¿resulta válido que la jurisprudencia española pueda, no sólo colmar esas reconocidas lagunas legales, sino incluso permitir injerencias en los derechos fundamentales a través de medidas de investigación no previstas legalmente?

4.2.1.1 La ilicitud de las escuchas domiciliarias

Con base legal en dicho art. 579 LECrim, existe un importante debate doctrinal en España en torno a la posibilidad de proceder a la interceptación de las conversaciones orales directas, precisamente con base legal en el archicitado art. 579 LECrim. Para los partidarios, en el concepto "comunicación" deben incluirse todo tipo de comunicaciones efectuadas por cualquier medio (telefax, ordenador, videófonos) y también el verbal, y no parece lógico afirmar la ausencia de regulación para grabar una conversación verbal directa, cuando lo sustantivo es el hecho de conversar y no el medio utilizado, de modo que cuando el legislador regula la intervención de las comunicaciones en el art. 579 LECrim, está dando por supuesto que se incluye la conversación oral, puesto que lo que se protege es la conversación en sí misma considerada[81]. Para los detractores, nuestro ordenamiento no prevé la posibilidad de intervenir las comunicaciones orales directas (salvo en la legislación penitenciaria), y ante la inexistencia de una norma habilitante con rango suficiente que permita legítimamente esta intervención, rige sin paliativos el derecho al secreto de tales comunicaciones e impide la obtención legítima del contenido de las mismas por un sujeto ajeno a la conversación[82].
Gracias a los avances tecnológicos, ya no es preciso acceder físicamente al interior de un domicilio para colocar micrófonos y aparatos de escucha para conocer las conversaciones que se mantengan dentro de aquél. Es lo que se denomina la «vigilancia

electrónico y proceso penal", *La Ley* nº5805, de 18 de junio de 2003, pp. 1 y ss.; MARCHENA GÓMEZ, M., "Dimensión jurídico penal del correo electrónico", *La Ley*, 4 de mayo de 2006, pp. 4-17; SÁNCHEZ NÚÑEZ, T., "Jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal", en VV.AA., *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 283.

[80] GIMENO SENDRA, V., "La intervención de las comunicaciones", *La Ley*, núm. 7192, de 9 de junio de 2009, p. 6.

[81] A favor, RAFOLS LLACH, J., "Autorización judicial para la instalación de aparatos de escucha, transmisión y grabación en lugar cerrado", *Cuadernos de Derecho Judicial*, CGPJ, Madrid, 1992, vol. I., p. 568; DÍAZ CABIALE, J. A., *La admisión y práctica de la prueba en el proceso penal*, ed. CGPJ, Madrid, 1991, p. 134; TORRES MORATO, M. A. (con DE URBANO CASTRILLO, E.) La *prueba ilícita penal: estudio jurisprudencial*, Editorial Aranzadi, 1997, p. 272; FÁBREGA RUIZ, C., "Secreto de las comunicaciones y proceso penal", *La Ley*, 1997-4, pp. 1187-1190; RIVES SEVA, A. P., *La intervención de las comunicaciones en el proceso penal. Análisis doctrinal, legislación y jurisprudencia*. Ed. Bosch, Barcelona, 2010, p. 283.

[82] En contra, JIMÉMEZ CAMPO, J., "La garantía constitucional del secreto de las comunicaciones", *Revista Española de Derecho Constitucional*, nº20, 1987, p. 63; LÓPEZ BARJA DE QUIROGA, J., *Las escuchas telefónicas y la prueba ilegalmente obtenida*, ed. Akal, Madrid, 1989, p. 183; ANDRÉS IBÁÑEZ, P., "Notas sobre la entrada y registro y la intervención telefónica", *Planes Provinciales y Territoriales de Formación*, vol. II, CGPJ, 1992, p. 1055; MORENO CATENA, V., "La intervención de las comunicaciones personales en el proceso penal", VV.AA., *La reforma de la Justicia penal: estudios en homenaje al Prof. Klaus Tiedemann*, Servicio de Publicaciones de la Universidad Jaume I, Castellón, 1997, p. 424; NOYA FERREIRO, M. L., *La intervención de las comunicaciones orales directas en el proceso penal*, ed. Tirant lo Blanch, Valencia, 2000, p. 126; CABEZUDO BAJO, M. J., *La inviolabilidad del domicilio y el proceso penal*, ed. Iustel, Madrid, 2004, p. 71 y ss.

acústica del domicilio» efectuada desde el exterior de aquél, prevista en el artículo 100.c) de la Ley de Enjuiciamiento Criminal alemana (StPO[83]); en los arts. 26 y siguientes de la RIPA en el Reino Unido; o en el art. 266 del Código Procesal Penal italiano.

Nuestro Tribunal Supremo se ha pronunciado en dos ocasiones con motivo de autorizar la instalación de aparatos de escucha y grabación en una celda para tomar conocimiento de las conversaciones orales entre dos presos[84], y en ambos casos su respuesta ha sido contundente: *"A este Tribunal no le resulta concebible que se proteja menos una conversación por ser telefónica -en cuanto pueda ser legítimamente intervenida por el Juez- y no lo pueda ser una conversación no telefónica de dos personas en un recinto cerrado"*. No obstante, en esta última sentencia de 2010 es preciso destacar el voto particular de los magistrados Perfecto Andrés Ibáñez y José Manuel Maza Marín, que advierten lo siguiente: «Cierto que en una interpretación hiperliteralista y deconstructiva del precepto en el término "comunicaciones", debidamente descontextualizado, caben las de cualquier tipo. Pero obrar así no es interpretar con rigor, y menos con el que exigen las normas de aplicación del *ius puniendi*; sino valerse de una clara e injustificable imperfección técnica del lenguaje legal para construir una norma contra la *ratio legis*: un *precepto no escrito de creación jurisprudencial.* Una regla tercera o supernumeraria que diga lo que no dice ninguna de los tomadas como supuesta base de la misma».

En nuestra opinión, el art. 579 LECrim no ampara la posibilidad de invasión de las comunicaciones entre sujetos presentes porque no concurre la debida previsión legal en los términos de "calidad" y "previsibilidad" exigible conforme al CEDH y a la jurisprudencia del TEDH. A pesar de que se ha defendido que existe jurisprudencia del TEDH que permite la posibilidad de tomar conocimiento de las conversaciones presenciales mediante la colocación de micrófonos en las dependencias de los centros penitenciarios[85], debemos advertir que la cobertura legal para legitimar las escuchas en los calabozos y centros penitenciarios constituiría una normativa especial para el entorno penitenciario que no sería en modo alguno aplicable a otros espacios cerrados (principalmente, los domicilios y aquellos otros lugares asimilados a aquéllos[86]), pues el ingreso en prisión de un ciudadano conlleva su inserción en un ámbito de intenso control público del que resulta la imposibilidad de generar un domicilio en el sentido constitucional del término[87].

[83]) Lo cual, en su día, originó un intenso debate doctrinal y jurisprudencial que incluso motivó la modificación de la Ley Fundamental alemana Véase la Sentencia del Tribunal Constitucional alemán de 30 de marzo de 2004 (BVerfGE 109, 279 –1 BvR 2378/98, 1 BvR 1084/99 –.

[84] SSTS de 10 de febrero de 1998 y de 2 de junio de 2010.

[85] Vid. DEL MORAL GARCÍA ("La intervención de las comunicaciones en centros penitenciarios", *La Ley*, núm. 7573, de 21 de febrero de 2011), quien cita las SSTEDH de 25 de septiembre de 2001 asunto P. G. y J. H. contra Reino Unido; 5 de noviembre de 2002 asunto Allan contra Reino Unido; 27 de abril de 2004, asunto Doerga contra Holanda; o 20 de diciembre de 2005, asunto Wisse contra Francia, y reconoce que "los problemas que se plantean en España son de previsión legal, pues el art. 579 LECrim no contempla claramente esa medida salvo que la entendamos comprendida en la vaga fórmula del inciso final del art. 579.3".

[86] Tanto el Tribunal Supremo como el Tribunal Constitucional han efectuado un concepto amplio y flexible del "domicilio", aunque lo fuera con carácter accidental o transitorio (habitaciones de hotel, autocaravanas, camarotes de embarcaciones, etc.).

[87] Vid. SSTC 22/1984, de 17 de febrero; 283/2000, de 27 de noviembre; y 89/2006, de 27 de marzo.

También debemos reiterar la reiterada exigencia de «calidad de la ley» por parte del TEDH, en el sentido de que exista una disposición legal expresa que así lo permita, cuando se trata de conocer lo que sucede en el interior de un domicilio. En un supuesto en el que un colaborador del acusado se presentó en su casa llevando escondido un aparato de radio-transmisión, gracias al cual la policía recibía y grababa la transmisión desde el exterior, el Tribunal Europeo declaró vulnerado el art. 8 CEDH porque la policía había grabado determinadas conversaciones del acusado en unas dependencias de su domicilio y *el poder discrecional legal que tenían las autoridades para prescribir la interceptación no estaba subordinado a ninguna condición y tanto el alcance como las modalidades de ejercicio de este poder no estaban definidas (...). En defecto de reglas específicas y detalladas, el recurso a esta técnica de vigilancia no se encontraba rodeada de las garantías adecuadas contra los diversos abusos posibles. Por ello, su puesta en práctica era susceptible de arbitrariedad e incompatible con la condición de legalidad*[88]. Es más, el caso más similar aplicable a la situación debatida en España es el caso *Vetter c. Francia* de 2005, referido a la autorización judicial para la entrada y colocación de micrófonos por la policía en un domicilio[89], y en el cual el TEDH también declaró la vulneración del art. 8 CEDH debido a la ausencia de regulación legal sobre la materia, pues la legislación francesa no preveía expresamente dicha medida de investigación. Para el TEDH, el hecho de que la legislación francesa permita la intervención de las comunicaciones emitidas o recibidas por medios telemáticos no resulta suficiente como base legal para proceder a la instalación de micrófonos en lugares privados por falta de "calidad de la ley", esto es, porque la ley debe utilizar términos lo suficientemente claros para que cualquiera comprenda en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a realizar dicho atentado secreto y virtualmente peligroso para el derecho al respeto de la vida privada y la correspondencia.

Los argumentos del TEDH pueden y deben ser alegados frente a quienes entienden que en España es posible la instalación de aparatos de escucha en los domicilios. Al igual que dicha medida no pudo adoptarse en Francia en virtud del art. 81 del CPP francés, que otorga al juez la potestad de acordar cualesquiera actuaciones útiles para la investigación del delito, relacionado con el art. 100 sobre la posibilidad de ordenar judicialmente la intervención de comunicaciones emitidas o recibidas por teléfono, fax, etc., tampoco podría adoptarse en España en virtud del art. 299 LECrim como cualesquiera actuaciones para averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación, y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos, ni en el art. 312 LECrim, que permite al juez de instrucción practicar cualesquiera medidas de investigación solicitadas en la querella, "salvo las que considere contrarias a las leyes, o innecesarias o perjudiciales para el objeto de la querella", relacionados con el art. 579 LECrim.

4.2.1.2 La ilicitud de los «programas troyanos» para el registro de dispositivos informáticos

[88] STEDH (Gran Sala) *Bykov c. Rusia,* de 10 de marzo de 2009, Demanda nº 4378/02, apartados 78 y ss.
[89] STEDH *Vetter c. Francia*, de 31 de mayo de 2005.

En nuestra opinión, el régimen legal del art. 579 LECrim tampoco resulta suficiente para acceder de manera remota a aquellos datos que, almacenados en la memoria de un equipo informático, no sean transmitidos a través de la Red. Como quiera que el equipo informático desde el cual se llevan a cabo las distintas actividades delictivas se ha convertido en un elemento probatorio casi indispensable para las autoridades encargadas de la investigación delictiva, y su análisis pericial en busca de los rastros digitales de sus actos se antoja esencial para lograr la condena penal de los autores de dichos delitos, se ha defendido la conveniencia de manejar *hardware* y *software* especializado, no sólo para la búsqueda y análisis de la información ocupada, sino también para poder acceder online a dicha información almacenada en la memoria del dispositivo, y ello como un importante y necesario avance tecnológico aplicable a la investigación criminal, a pesar de la desfasada regulación legal al respecto, que alude al registro de «libros y papeles[90]».

Cualquier ciudadano puede adquirir en el Mercado diversos programas informáticos denominados «espías» o «troyanos[91]», que pueden ser instalados de forma remota desde otro ordenador y que, una vez instalados, permiten grabar no sólo todo lo tecleado en el ordenador, sino también todos los correos electrónicos, conversaciones de chats y sitios visitados, y enviar informes periódicos de la actividad o la propia información a una cuenta de correo electrónico previamente configurada. También es cierto que en otros Ordenamientos jurídicos se ha admitido como medida de investigación los denominados «registros remotos» (o registros *online*), que permiten a las autoridades responsables de la investigación escanear su disco duro y demás unidades de almacenamiento y remitir de una manera remota y automatizada el contenido del mismo a otro equipo informático (el de la autoridad responsable de la investigación).

En España, se ha defendido una interpretación jurisprudencial integradora de los requisitos constitucionales y legales necesarios para legitimar el registro remoto de equipos informáticos, a partir de la aplicación analógica de los presupuestos, condiciones y garantías exigibles respecto de la entrada y registro, la ocupación de documentos, la detención de la correspondencia y de las intervenciones telefónicas[92]. Es más, el propio Tribunal Constitucional (STC 173/2011) abre la puerta a la posible admisibilidad de esta injerencia, pues da por hecho que los registros de equipos informáticos puedan llevarse a cabo en un futuro "ya sea por vía de acceso remoto a través de medios técnicos, ya, como en el presente caso, por vía manual".

Pero en nuestra opinión, estas interpretaciones no pueden suplir la necesidad de una *lex scripta, lex stricta* y *lex praevia*. No es posible justificar el empleo de cualesquiera métodos de investigación, sin una mínima base legal que regule sus garantías, requisitos y límites, bajo la excusa de poder contrarrestar así los avances con los que cada día cuentan los criminales para cometer sus delitos[93], de modo que, a pesar de las carencias

[90] Vid. SSTS de 18 de mayo de 2001 y de 14 de febrero de 2006.
[91] Por ejemplo, los programas *e-blaster*, *Perfect keylogger*, *TeamViewer*, o *GoToMyPC*.
[92] A favor de la utilización de los programas de tipo *keylogger* y *eblaster* en la investigación penal, vid. URBANO DE CASTRILLO, E., "La investigación tecnológica del delito", URBANO DE CASTRILLO, E., "La investigación tecnológica del delito", en VV.AA.: Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 65, y VELASCO NÚÑEZ, E., *Delitos cometidos a través de Internet. Cuestiones Procesales,* ed. La Ley, Madrid, 2010, p. 131.
[93] Para VELASCO NÚÑEZ ("Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos", en VV.AA., *Los nuevos medios de investigación en el*

de la regulación legal, debamos resignarnos a su utilización de la forma más racional posible para no obstaculizar grave e injustificadamente la investigación penal. La respuesta del Estado de Derecho debe ser la reforma del ordenamiento jurídico que garantice los principios de legalidad y seguridad jurídica, pues resulta indispensable que *las normas sean claras y detalladas, tanto más cuanto que los procedimientos técnicos utilizables se perfeccionan continuamente*[94], de modo que no consideramos posible una aplicación analógica de la regulación establecida respecto de otras medidas de investigación que puedan guardar cierta relación con dicho registro, ante la inexistencia de una norma legal especial habilitante de este tipo de injerencias, problema incluso reconocido por los partidarios de la admisibilidad de dicha medida[95].

4.2.2 El debate sobre la judicialidad: la admisibilidad de la injerencias policiales "leves" sin orden judicial previa

El derecho fundamental al secreto de las comunicaciones sólo puede ser limitado mediante resolución judicial, y además, se trata de un derecho "de contenido formal", en el sentido de que la protección dispensada por el art. 18.3 CE se extiende también a la libertad de comunicación, esto es, "*se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de la persona, lo íntimo o lo reservado. Por ende, el secreto ha de salvaguardarse tanto en los casos en que pueda comprenderse en el ámbito de la intimidad o de la vida privada, como en aquellos casos en que la comunicación no afecte a dicha esfera*" (STC 114/1984, y tal y como advirtió el TEDH en el caso *Malone*). Por ello, se entiende que el concepto de secreto de la comunicación no sólo cubre su contenido, sino otros aspectos de la comunicación, como la identidad subjetiva de los interlocutores y demás circunstancias o datos externos de la conexión telefónica: su momento, duración y destino, etc.

Ahora bien, la solución ofrecida por el TEDH en el caso *Malone*, tanto por su singularidad, como por el estado de los avances técnicos en la fecha en que aquélla fue pronunciada, sólo pudo referirse a algunos datos muy concretos relacionados con la técnica del recuento —*pen register* o *comptage*—. Hoy en día, la telefonía móvil o las comunicaciones electrónicas a través de Internet generan toda una serie de datos de tráfico que van mucho más allá de aquéllos respecto de los que el TEDH tuvo ocasión de pronunciarse en 1984. Por ello, el Tribunal Supremo español ha afirmado que *el concepto de «datos externos» manejado por el TEDH en la tantas veces invocada*

---

proceso penal. Especial referencia a la tecnovigilancia, Cuadernos de Derecho Judicial, 2007-II, CGPJ, p. 107), "los instrumentos de trabajo de la policía deben ponerse a la altura de los tiempos y entenderse que el ejercicio de las facultades legales que les procura el art. 22.2 LOPDP y el 12.3 LSSICE son autónomamente compatibles con la supervisión judicial de los Derechos Fundamentales del investigado, y la corrección a los hipotéticos excesos, fraudes o posibles abusos que pudieran darse, encontrarla más bien en la responsabilidad penal o disciplinaria del concreto investigador, que en la forzada nulidad probatoria (que más que corregir futuras actuaciones policiales, aboca en impunidades intolerables y en "castigos" a la inocente Sociedad que debe soportarlas)".

[94] Vid. SSTEDH *Kruslin* y *Huvig c. Francia* de 24 de abril de 1990: "la ley debe ser lo suficientemente clara para señalar a todos las circunstancias y condiciones en que autoriza a los poderes públicos a recurrir a una injerencia así, secreta y posiblemente peligrosa, en el derecho al respeto de la vida privada y de la correspondencia". Esta afirmación la consideramos perfectamente predicable del entorno digital.

[95] VELASCO NÚÑEZ, E., "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal", *La Ley Penal*, núm. 82, 2011, pág. 24.

sentencia del Caso Malone, ha sido absolutamente desbordado por una noción más amplia, definida por la locución «datos de tráfico», en cuyo ámbito se incluyen elementos de una naturaleza y funcionalidad bien heterogénea[96].

El actual debate doctrinal y jurisprudencial en torno a la necesidad de contar con una orden judicial previa para proceder a la obtención de determinados datos referidos a ciertas comunicaciones electrónicas se centra en la naturaleza de los datos a los que se pretende acceder, pues no es lo mismo entender afectado el Derecho Fundamental a la intimidad (art.18.1 CE) que el Derecho al secreto de las comunicaciones (art. 18.3 CE), como ya se ha advertido. En primer lugar, el derecho al secreto de las comunicaciones "alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos, de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación". En segundo lugar, no existe en la Constitución reserva absoluta de previa resolución judicial respecto del derecho a la intimidad personal, de modo que aunque se ha reconocido también respecto del derecho a la intimidad personal, como regla general, la exigencia de monopolio jurisdiccional, se ha admitido de forma excepcional *que en determinados casos y con la suficiente y precisa habilitación legal sea posible que la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas*, siempre que respeten las exigencias dimanantes del principio de proporcionalidad y existan razones de urgencia y necesidad que motiven la intervención policial inmediata. Y en tercer lugar, es doctrina sólida aquélla según la cual el conocimiento y uso de los datos de tráfico supone una «injerencia de menor intensidad[97]» en el Derecho al Secreto de las Comunicaciones del art. 18.3 CE, que el conocimiento del contenido de las mismas.

Pues bien, el resultado de esta doctrina, que enfatiza esa falta expresa de una reserva jurisdiccional en el art. 18.1 CE para admitir supuestos excepcionales de intervención policial sin autorización judicial previa, encuentra su mejor exponente en la jurisprudencia referida a la obtención policial de los códigos IMSI e IMEI o la captación policial de los datos de localización emitidos por determinados aparatos, como ya hemos explicado anteriormente[98], así como la tolerancia de indagaciones policiales sin orden judicial previa sobre la «agenda de contactos» de los teléfonos móviles, al considerar el Tribunal Supremo que dicho acceso no afecta al derecho al secreto de las comunicaciones (como sí sucede si se accede al «listado de llamadas»), sino, todo lo más, frente a la infracción del derecho a la intimidad del investigado, pues la agenda de un teléfono móvil "es equiparable a una agenda en soporte de papel o electrónica con el mismo contenido de direcciones y números de teléfono[99].

[96] Vid., por todas, la STS núm. 249/2008, de 20 mayo de 2008.
[97] Vid. SSTC 123/2002 y 26/2006: *aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las «escuchas telefónicas», siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad*.
[98] Véase el apartado 3.3.2.
[99] SSTS de 27 de junio de 2002; 25 de julio y 25 de septiembre de 2003; 1 de marzo, 26 de abril y 25 de mayo de 2011. Por el contrario, el examen policial de las llamadas entrantes y salientes fue prohibido tras la STC 230/2007, de 5 de noviembre de 2007, y dicha doctrina ha sido posteriormente reconocida por el

Ahora bien, esta doctrina diferenciadora entre la afectación al secreto de las comunicaciones y a la intimidad puede no resultar fácil de aplicar en la práctica, debido precisamente a la continua evolución de la tecnología. Si la información a aprehender se halla en el disco duro de un equipo informático localizado en un domicilio, es evidente que se encuentra protegida por las garantías y requisitos establecidos para la protección de la inviolabilidad del domicilio (art. 18.2 CE), pero ¿y si se localiza en el disco duro de un ordenador portátil o un teléfono móvil?, ¿puede la policía, con ocasión de efectuar un cacheo a un transeúnte y ocuparle un dispositivo electrónico (memoria USB, *tablet*, *Smartphone*, etc.) examinar el contenido de la memoria del aparato que el sujeto lleva consigo? Recordemos que la regla general a seguir, según la STC 173/2011, debe ser la autorización judicial a la hora de inspeccionar la memoria de un ordenador, salvo si existen razones de necesidad y urgencia y el acceso policial respeta los principios de proporcionalidad y razonabilidad.

Debido a la extraordinaria cantidad y diversidad de información almacenable en los actuales dispositivos electrónicos que una persona puede llevar consigo, consideramos que resultaría desproporcionado amparar tal registro bajo el clásico "cacheo" o en la ocupación de objetos que se deriva de la detención policial[100]. Basta indicar que los libros en formato electrónico que pueden almacenarse en una tarjeta de memoria inserta en un teléfono móvil supondrían varios miles de páginas si fueran impresos en papel. Por lo tanto, el acceso a la información contenida en cualquier dispositivo electrónico o informático no puede ser considerado como una injerencia "leve" en la esfera de la privacidad de las personas, equiparable al examen de cartas, papeles, agendas o mochilas.

4.2.3 El debate sobre la motivación judicial: la obtención de nuevos formatos de información y nuevos datos derivados de las comunicaciones

El requisito de la exclusividad jurisdiccional conduce a la exigencia de que se dicte una resolución judicial previa y que ésta sea motivada pues los tribunales han tenido muy claro desde el principio que la falta de motivación de la resolución judicial que restrinja un derecho fundamental infringe la proporcionalidad de la medida, y en su caso, el derecho a la tutela judicial efectiva[101]. Tal y como se advirtió en la STC 86/1995, de 6 de junio, la existencia de un mandamiento judicial autorizando la intervención de la comunicación, junto con la estricta observancia del principio de proporcionalidad en la ejecución de esta diligencia de investigación, *constituyen exigencias constitucionalmente inexcusables que afectan al núcleo esencial del derecho al secreto de las comunicaciones, de tal modo que la ausencia de autorización judicial o la falta de motivación determinan, irremediablemente, la lesión del derecho constitucional* y, por lo tanto, la prohibición de valoración de cualquier elemento probatorio que pretenda deducirse del contenido de las conversaciones intervenidas, no sólo del resultado mismo

Tribunal Supremo en las SSTS de 8 de abril y 14 de mayo de 2008, 18 de diciembre de 2009 y 12 de diciembre de 2010.

[100] Vid. GONZÁLEZ-CUÉLLAR SERRANO ("Garantías Constitucionales…", op. cit., p. 915) y KERR ("Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", July 2002, p. 22).

[101] STC 62/1982, de 15 de octubre.

de la intervención, sino de cualquier otra prueba derivada de la observación telefónica, siempre que exista una conexión causal entre ambos resultados probatorios[102].

En concreto, la motivación de cada autorización judicial que ordene la interceptación de una comunicación debe mencionar expresamente, no solamente los hechos investigados y las razones de hecho y jurídicas que apoyan la necesidad de hacerla, *sino también determinar con precisión su objeto (especialmente, la línea o líneas telefónicas intervenidas, las personas cuyas conversaciones han de ser interceptadas, la duración de la medida y quién y cómo ha de llevarse a cabo)*[103]. Ahora bien, esta idea referida a las escuchas telefónicas debe ser ampliada cuando se trata de comunicaciones electrónicas, pues en el primer caso lo importante era conocer el contenido de la conversación oral, los números de teléfono involucrados en dicha conversación, y el momento en que se produjo la misma. Por el contrario, cuando se trata de comunicaciones electrónicas, surgen muchísimos otros datos de enorme valor para las labores de investigación criminal (por ej., el lugar geográfico desde donde se produjo el envío de un SMS o el momento y lugar exacto en donde se encendió o desconectó el teléfono móvil).

El problema reside en que la jurisprudencia española ha declarado reiteradamente que el conocimiento y uso de los datos de tráfico supone una «injerencia de menor intensidad[104]» en el Derecho al Secreto de las Comunicaciones del art. 18.3 CE que el conocimiento del contenido de las mismas, y como consecuencia de dicha interpretación, se ha llegado al extremo de defender que *esa menor intensidad debe proyectarse en un doble campo: en relación a la petición policial la entidad de los datos justificativos de la petición pueden ser menos intensos, y en relación a la autorización judicial, ésta puede serlo por providencia que, como se sabe no exige una motivación específica, bastando la remisión al oficio*[105].

Sin embargo, consideramos que el acceso a determinados datos "externos" o "de tráfico" generados con motivo de una comunicación no tiene por qué estimarse, automáticamente, una menor injerencia que el acceso al contenido comunicativo sin más. El acopio, tratamiento y uso de determinados datos generados con motivo de las comunicaciones electrónicas constituyen una vital y suculenta fuente de información, mucho más importante que el acceso al contenido mismo de la conversación. Así, por ejemplo, para las autoridades encargadas de la investigación puede resultar muchísimo más importante conocer la dirección IP utilizada, la fecha y la hora de la conexión y desconexión del servicio de acceso a Internet registradas, o la información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y

[102] Doctrina reiterada en las SSTC 181/1995, de 11 de diciembre; 49/1996, de 26 de marzo; 54/1996, de 26 de marzo; 123/1997, de 1 de julio; 49/1999, de 5 de abril; 166/1999, de 27 de septiembre; 171/1999, de 27 de septiembre; 236/1999, de 20 de diciembre; 126/2000, de 16 de mayo; 14/2001, de 29 de enero; 202/2001, de 15 de octubre; 82/2002, de 22 de abril; 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre; 205/2005, de 18 de julio; 259/2005, de 24 de octubre; 104/2006, de 3 de abril; ó 239/2006, de 17 de julio.

[103] Vid. SSTC 261/2005, de 24 de octubre, y 236/1999, de 20 de diciembre.

[104] Vid. SSTC 123/2002 y 26/2006: *aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las «escuchas telefónicas», siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad*.

[105] STS núm. 737/2009, de 6 de julio.

de la del destino de la llamada, que el conocimiento de la conversación mantenida por el sospechoso. De ahí que, si se analiza detenidamente la dimensión cuantitativa y cualitativa de los datos enumerados en el art. 3 de la LCDCE y en el art. 33 LGT, resulta fácil deducir que la información que puede arrojar la obtención, análisis y cruce de tales datos puede llegar a ser infinitamente superior al propio contenido de la comunicación. En una Sociedad en la que la información más íntima, confidencial y reveladora de la personalidad de un individuo ya no se guarda en cajones ni armarios, sino en la memoria de un PC y en bases de datos alojadas en servidores, resulta factible considerar que el acceso a determinados datos de tráfico y el uso cruzado entre los mismos puede significar una invasión en nuestra intimidad muchísimo más intrusiva que la propia entrada y registro de nuestros domicilios o el conocimiento del contenido de nuestras conversaciones, pues a través del cruce de determinados datos generados a partir de las comunicaciones, puede extraerse el tan temido «perfil detallado de la personalidad» de un sujeto.

En contra de lo sustentado por los tribunales españoles, estimamos que el uso en profundidad, de modo sistemático y cruzado, de los datos de tráfico puede suponer en ciertas ocasiones una injerencia en la privacidad de las personas mucho mayor que el acceso al contenido de una conversación. Así lo declaró el Tribunal Constitucional alemán en su Sentencia de 2 de marzo de 2010[106], al pronunciarse sobre la constitucionalidad de la reforma de la Ley de Telecomunicaciones alemana (TKG), en donde señaló como *los datos de tráfico almacenados no pueden, junto con otros datos existentes o disponibles, permitir la reconstrucción de prácticamente todas las actividades de los ciudadanos. La importancia de estos datos es de gran alcance porque, dependiendo de la utilización de los servicios de telecomunicaciones, los datos de tráfico -y, sobre todo, si sirven como punto de partida para nuevas investigaciones- pueden arrojar un profundo conocimiento del entorno social y las actividades individuales de cada ciudadano* (F.J. núm. 211). De esta manera, el Tribunal Constitucional germano llegó a una conclusión trascendental que contradice la posición actual de la doctrina y jurisprudencia española: *Puesto que un análisis de estos datos permite penetrar profundamente en la vida privada y en algunos casos extraer conclusiones más detalladas acerca de la personalidad y permite incluso los perfiles de movimiento de una persona, no se puede suponer sin más, como hasta el momento, que el uso de esta información general tiene una menor injerencia que la interceptación del contenido de una comunicación* (F. J. núm. 227).

En conclusión, cabe afirmar que "intervenir un teléfono no es lo mismo que intervenir un teléfono más todos los datos de identidad, sms, listado de llamadas, correos electrónicos, ubicación geográfica, etc., que automáticamente facilita el sistema y obligatoriamente ha de ceder el operador. En este aspecto, la nueva tecnología permite una inmisión en la intimidad (en sentido amplio) mucho más potente que la que suponía el clásico «pinchazo», lo que no puede quedar extramuros de la exigencia de ponderación que se imponía al juez en el marco analógico[107]".

En consecuencia, habrá de tenerse presente la necesaria relación que ha de existir entre motivación y proporcionalidad, en los términos expresados en el conocido ATS de 18

[106] Sentencia de la Sala Primera. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), que resuelve los procesos BvR 256/08, 263/08 y 586/08.
[107] CRESPO BARQUERO, P., "Intervenciones judiciales en materia de comunicaciones telefónicas e Internet", *Cuadernos Penales José María Lidón*, núm.7/2010, p. 92.

de junio de 1992: «A mayor trascendencia de la decisión, mayor exigencia, si cabe, respecto de la motivación». Y de ahí la crítica vertida por Marchena Gómez con respecto a la actual redacción del art. 33 LGT, por cuanto "la injerencia de los agentes de policía, en unos casos, en el derecho a la inviolabilidad de las comunicaciones, en otros, en el derecho a la protección de datos, no es el resultado de un acto jurisdiccional que pondere los bienes jurídicos en juego y decida el sacrificio de aquéllos, sino de una previsión normativa impuesta con carácter genérico a las operadoras de telefonía que, sea cual sea la gravedad del delito investigado, estén o no en juego el principio de proporcionalidad y otros bienes jurídicos que justifiquen el sacrificio, va a imponer, por ministerio de la Ley, la disponibilidad de esos datos electrónicos a favor de la fuerza pública investigadora[108]".

Para Marchena Gómez, "las singularidades impuestas por la evolución de las comunicaciones telefónicas y telemáticas, están demandando de nuestra jurisprudencia una atención renovada que supere nuestro anclaje histórico en una forma de concebir las exigencias de motivación que ha sido desbordada por los avances tecnológicos". No sólo debería analizarse la suficiencia o insuficiencia del auto habilitante desde la perspectiva de la valoración de los indicios ofrecidos por la policía, sino que también debería analizarse la motivación respecto a la cualidad y naturaleza de la información solicitada, pues la investigación penal de un delito grave no tiene por qué conllevar, siempre y en todo caso, la máxima intensidad en el sacrificio de los derechos fundamentales que convergen en el momento de cualquier comunicación telefónica o telemática. Si los agentes facultados, además de acceder al contenido de las conversaciones, pretenden tener conocimiento de esa otra información (por ejemplo, su ubicación geográfica en el momento de realizar o recibir una determinada llamada), han de explicar al órgano jurisdiccional qué singularidades de la investigación imponen ese añadido menoscabo en el círculo de derechos fundamentales del imputado. Y el órgano jurisdiccional ha de incluir en su fundamentación jurídica un razonamiento acerca del espacio abarcado por la injerencia, qué datos han de ser objeto de interceptación, a qué formato de comunicación electrónica se extiende la autorización para la cesión de los datos, y deberá, además, justificar la necesidad de la decisión a la vista de la información ofrecida por las fuerzas de seguridad respecto de la funcionalidad de los datos. Lo contrario supone lanzar una suerte de "red de arrastre digital" no conforme con la debida motivación y ponderación de los intereses en juego.

4.2.4 El debate sobre la proporcionalidad: La noción de "delito grave" legitimador del uso de medidas tecnologías de investigación

El cuarto y último debate guarda relación con uno de los motivos por los que el TEDH condenó en dos ocasiones a España en materia de escuchas telefónicas, pues para el tribunal europeo la regulación española no establecía "ni la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial, ni la naturaleza de las infracciones a que puedan dar lugar". A partir de entonces, los tribunales españoles han exigido imperativamente que la limitación del derecho al secreto de las comunicaciones sólo puede tener lugar con motivo de la investigación

[108] MARCHENA GÓMEZ, M., "La vulneración de derechos fundamentales por ministerio de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones)", *La Ley*, núm. 7572, de 18 de febrero de 2011. Dicha crítica también ha sido expuesta en varios votos particulares. En concreto, véanse sus votos particulares a las SSTS de 6 de octubre de 2011 y de 20 de enero de 2012.

penal de un «delito grave». De hecho, el principal objetivo de la aprobación de la LCDCE de 2007 es conservar determinados datos relativos a las comunicaciones electrónicas con el fin de ser cedidos a las autoridades responsables de una investigación criminal "con fines de detección, investigación y enjuiciamiento de *delitos graves* contemplados en el Código Penal o en las leyes penales especiales". Ahora bien, ¿qué se entiende en España por "delito grave"?

Aunque el Código Penal español tipifica como delitos graves los que llevan aparejada una pena de prisión superior a los 5 años, así como una pena privativa de derechos superior a 5 años, el concepto de "delito grave" manejado en el ámbito procesal para restringir derechos fundamentales es distinto. Así, por ejemplo, para acordar la prisión provisional de un sospechoso, el art. 503 LECrim exige que el delito esté castigado con pena igual o superior a la de dos años de prisión, e incluso menos, cuando el imputado contara con antecedentes penales no cancelados o que pudieran serlo derivados de delitos dolosos. Para legitimar la utilización del agente encubierto como medida excepcional de investigación, el art. 282 bis LECrim autoriza su empleo para investigaciones que afecten a actividades propias de la delincuencia organizada, enumerando un listado de delitos que pueden ser cometidos por la delincuencia organizada[109]. Y para proceder a la inclusión de las muestras de ADN de un persona en las bases de datos policiales, el art. 3 de la L.O. 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, establece un catálogo, aunque escueto y genérico, de los supuestos en los que se permite la inscripción de los datos identificativos extraídos a partir del ADN en el marco de una investigación criminal[110]. Es más, la punibilidad necesaria para que un hecho tenga la consideración de "delito grave" es incluso menor en determinadas Directivas y Decisiones Marco europeas. Así por ejemplo, el art. 2.1 de la Decisión Marco de 2002 relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros[111] permite dictar una orden de detención europea por "aquellos hechos para los que la ley del Estado miembro emisor señale una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de 12 meses o, cuando la reclamación tuviere por objeto el cumplimiento de condena a una pena o medida de seguridad no inferior a cuatro meses de privación de libertad". Y el art. 3.5.f) de la Directiva de 2005 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo[112] considera como «delitos graves», entre otros, "los delitos que lleven aparejada una pena privativa de libertad o medida de seguridad de duración máxima superior a un año o, en los Estados en cuyo sistema jurídico exista un umbral mínimo para los delitos, todos los delitos que lleven

[109] Ese listado del art. 282 bis LECrim ha sido propuesto jurisprudencialmente como catálogo de delitos a la hora de justificar la interceptación de las telecomunicaciones. Véanse la STS de 8 de julio de 2000 y la STS de 22 de enero de 2003.

[110] Según el art. 3.1.a), debe tratarse de "delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados".

[111] Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DOUE L 190, de 18.7.2002).

[112] Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo (DOUE L 309, de 25.11.2005).

aparejada una pena privativa de libertad o medida de seguridad de duración mínima superior a seis meses".

En otros Ordenamientos jurídicos, la posibilidad de acordar la interceptación de las telecomunicaciones depende, bien de que el hecho investigado se corresponda con un determinado listado de delitos, o bien en atención de la pena[113]. Pero nada de esto se establece en el ordenamiento español, en donde nuestros tribunales valorar la gravedad del delito, no exclusivamente en atención a la pena con la que el mismo se sanciona, sino también en atención a otros criterios tan diversos como el "bien jurídico protegido"; la "trascendencia y repercusión social" de los hechos, o el hecho de que sean organizaciones complejas las que se dedican a su comisión[114]. Y a partir de la STC 104/2006, también se considera igualmente un criterio válido a la hora de entender que nos encontramos ante un *delito grave,* a efectos de legitimar el recurso a la limitación del derecho fundamental al secreto de las comunicaciones, la «incidencia del uso de las tecnologías de la información, tanto para la perpetración del delito como para la obstrucción a su persecución» al admitirse la idoneidad de determinadas medidas de investigación basadas en las TIC para investigar aquellos delitos perpetrados a través o con ayuda de las telecomunicaciones[115].

En la actual Era Digital, resulta cada vez más indispensable el empleo de especiales medidas tecnológicas de investigación para logar una persecución eficaz de aquellos delitos que se aprovechen, en sus diversas modalidades comisivas, de las ventajas que se deducen del uso de las nuevas tecnologías, sobre todo con motivo del entorno virtual en el cual pueden llegar a cometerse. Por tanto, cuando se trata de delitos ejecutados mediante instrumentos electrónicos, en un medio digital, o cuyas evidencias también presentan un formato digital, la obtención de pruebas puede exigir necesariamente el empleo de especiales medidas de investigación, y en este punto, la interceptación de las comunicaciones electrónicas o la obtención de determinados datos generados con motivo de las mismas juega un papel trascendental y necesario.

Así, por ejemplo, para la investigación de unas injurias graves o unas amenazas efectuadas a través de las Redes sociales, la identificación del titular desde cuya IP se efectuaron tales manifestaciones exigirá la solicitud de determinados datos a las operadoras de telecomunicaciones y prestadoras de servicios de Internet. Como bien se recoge en el AAP de Valencia de 7 de junio de 2011, "aunque los delitos investigados no lleven aparejadas penas que tengan la consideración de graves, no podemos dejar de

[113] Así, por ejemplo, los arts. 100a y ss. del Código Procesal Penal alemán establecen un amplio catálogo de delitos considerados "graves" o de "especial trascendencia" y respecto de los cuales se pueden utilizar diversas medidas de investigación y prueba, como la interceptación de las telecomunicaciones. El Código francés autoriza en su art. 100 la interceptación, la grabación y la transcripción de las telecomunicaciones, cuando se trate de delitos cuya pena prevista fuera igual o superior a dos años de prisión. Y finalmente, el art. 266 del Código italiano establece un sistema mixto, pues por una parte recoge una catálogo de figuras delictivas respecto de las cuales se puede utilizar como método de investigación y prueba, la interceptación de las comunicaciones telefónicas, así como una cláusula general en virtud de la cual dicha medida es también admisible cuando se trate de delitos en los que la pena prevista sea igual o superior a cinco años de prisión.

[114] Como estudio en particular de la jurisprudencia referida a la noción de "delito grave" necesaria para acordar la interceptación de las comunicaciones, vid. RODRÍGUEZ LAINZ, J. L., "Hacia un nuevo entendimiento del concepto de gravedad del delito en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas", *Diario La Ley*, nº7789, de 2 de febrero de 2012. Versión electrónica disponible en: http://diariolaley.laley.es.

[115] STC 104/2006, de 3 de abril, F. J. 4º.

lado otras conductas que de otro modo sería imposible su persecución, puesto que muchos de los delitos producidos a través de la red requieren de una averiguación de las direcciones de IP de los ordenadores desde donde se han producido, datos que tan solo pueden ser investigados accediendo a la información que conservan las operadoras del servicio (…). Es más, la última modificación del Código Penal, introduce nuevos delitos realizados a través de Internet como el regulado en el art. 183 bis llamado *ciberacoso*, que está penado con pena entre 1 y 3 años de prisión o multa, que por sus penas podría entenderse como delito menos grave, pero que no tiene otra forma de investigarse que a través de la averiguación de las direcciones IP de los ordenadores desde donde se produjeron las comunicaciones[116]".

El lado positivo de esta interpretación abierta por la que se ha optado en España es que resulta propicia para asumir la actual corriente expansiva de la noción de «delito grave» procedente la Unión Europea, a los efectos de legitimar la utilización de especiales medidas tecnológicas de investigación limitativas de derechos fundamentales (v. gr., interceptación de las comunicaciones, registros remotos o seguimientos electrónicos) para garantizar una persecución eficaz de los delitos que son objeto de regulación por parte de la Unión Europea, bien porque puedan tener cierta trascendencia transnacional, bien porque se estimen que constituyen supuestos de "delincuencia grave". Así sucede, por ejemplo, con las recientes Directivas de la Unión Europea en materia de lucha contra la trata de seres humanos, protección de las víctimas y los atentados contra la libertad sexual de menores de edad y la pornografía infantil[117], que no se limitan a señalar aquellas infracciones que deberán ser tipificadas por los Estados miembros, sino que instan a éstos a adoptar "las medidas necesarias para garantizar que las personas, unidades o servicios responsables de la investigación o del enjuiciamiento (…) dispongan de «instrumentos de investigación eficaces», tales como los que se utilizan contra la delincuencia organizada y en otros casos de delincuencia grave", y entre los que se cita expresamente la interceptación de comunicaciones.

[116] AAP núm. 379/11, secc. 16ª, de 7 de junio de 2011.

[117] Directiva 2011/36/UE, del Parlamento Europeo y del Consejo, de 5 abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión Marco 2002/629/JAI (relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión marco 2002/629/JAI del Consejo (DOUE L 101, de 15 de abril de 2011) y Directiva 2011/92/UE, del Parlamento Europeo y del Consejo, relativa a la lucha contra los abusos sexuales y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI, del Consejo (DOUE L 335, de 17 de diciembre de 2011).

5

Conclusiones y propuestas de reforma

1.

La tecnología debe ser utilizada en la investigación criminal al igual que es empleada en cualesquiera ámbitos de nuestra sociedad moderna, pues tal y como anticipó el magistrado Ruiz Vadillo en 1988, "las innovaciones tecnológicas -el cine, el video, la cinta magnetofónica, los ordenadores electrónicos, etc.- pueden y deben incorporarse al acervo jurídico procesal en la medida en que son expresiones de una realidad social que el derecho no puede desconocer118". Pero no es posible justificar el empleo de cualesquiera métodos de investigación, sin una mínima base legal que regule sus garantías, requisitos y límites, bajo la excusa de poder contrarrestar así los avances con los que cada día cuentan los criminales para cometer sus delitos.

En España existe una completa unanimidad en cualquier foro jurídico sobre la conveniencia de reformar nuestra legislación procesal penal, y a la hora de actualizar nuestra vetusta Ley de Enjuiciamiento Criminal, es preciso actualizar el catálogo y régimen jurídico de las medidas de investigación de conformidad con las modernas técnicas que proporcionan los avances tecnológicos. Pero no basta con cualquier previsión legal genérica o meramente enunciativa de las medidas a acordar para estimar cumplido el principio de legalidad; la normativa reguladora de dichas diligencias de investigación deberá ser una normativa "de calidad y claridad", tal y como requiere la doctrina emanada del TEDH, que exige que las normas estén redactadas con la suficiente precisión como para permitir al individuo regular su conducta conforme a ella y predecir las consecuencias de la misma. Por lo tanto, la futura Ley española deberá regular expresamente diligencias de investigación hasta ahora atípicas en nuestra legislación (por ej., las vigilancias acústicas), así como precisar los límites y concretar los requisitos de las ya previstas, aunque de modo insuficiente (por ej., las escuchas telefónicas o las pruebas de ADN), esto es, definir con claridad las modalidades y extensión del ejercicio del poder otorgado a las autoridades, los supuestos en los que se legitime su utilización, los sujetos sobre los que puedan acordarse tales medidas, su duración máxima, etc. Todo ello debido a que, sin perjuicio de que la jurisprudencia pueda colmar las lagunas legales, no puede desembocar en una suerte de "creación judicial del Derecho" en la que actualmente nos encontramos, permitiendo nuevas injerencias en los derechos fundamentales a través de medidas de investigación no previstas legalmente. Por ello, a pesar de que el TEDH haya legitimado el régimen de las escuchas telefónicas complementado por la jurisprudencia española, ha llegado el momento de abordar la necesaria reforma de la legislación procesal para poder emplear en nuestro país en las tareas de investigación criminal, con las debidas garantías, los instrumentos de vigilancia electrónica, con especial atención a aquellos delitos en los

[118] STS, sala penal, de 5 de febrero de 1988.

que la informática y las TIC juegan un papel muy importante (muy especialmente, la ciberdelincuencia).

2.

La regulación de las medidas de investigación relacionadas con el uso de la tecnología utilizables en la persecución criminal debe tener presente el grado de injerencia que el desarrollo tecnológico en la utilización de tales instrumentos pueden producir en la afectación a los derechos fundamentales de los sujetos investigados, y dicha injerencia debe ser valorada, no sólo desde un punto de vista cualitativo (v. gr., en virtud de la naturaleza del instrumento tecnológico utilizado), sino también desde un punto de vista cuantitativo (v. gr., en función de la duración de su utilización), para evitar incurrir en un exceso. Por ello, dicha regulación legal habrá estar presidida por los principios de necesidad, idoneidad, proporcionalidad y prohibición de exceso, de conformidad con la doctrina reiterada del TC y TEDH.

Además, a la hora de procederse a efectuar dicha regulación, se deberá tener presente la continua evolución científica (por ej., a la hora de regular el cotejo de voces o escritura del acusado) y permitir ciertos márgenes de apreciación judicial en función de las circunstancias de cada caso, tratando de no contener una regulación excesivamente minuciosa que pueda dar lugar a una obsolescencia casi inmediata a su entrada en vigor.

3.

En particular, el actual régimen de la intervención de las comunicaciones (de todo tipo, y especialmente las electrónicas) debería reformarse inmediatamente para cumplir las exigencias establecidas por la jurisprudencia del TEDH y del TC español. No hay que olvidar que hasta el propio presidente de la Audiencia Nacional ha reclamado la necesidad de aprobar una Ley Orgánica que regule de un modo detallado la problemática surgida en torno a la intervención de las conversaciones telefónicas para prestar una mayor seguridad jurídica a los ciudadanos, a los acusados y a los propios jueces, "para saber -los magistrados- hasta donde podemos llegar y qué límites no podemos sobrepasar[119]".

Por lo tanto, debe cesar la desidia del legislador español en su deber de adaptar la legislación procesal a la actual *Era digital* y a los desafíos que plantean las nuevas tecnologías, máxime si tenemos presente que la labor interpretativa de los tribunales debiera ser, en todo caso, complementaria y no sustitutiva de una regulación legal de la tipología de medidas legales de investigación relacionadas con la Informática, su alcance, requisitos y garantías.

4.

Junto con la necesaria regulación procesal de los requisitos necesarios para permitir la interceptación de las comunicaciones de cualquier clase que se realicen a través de cualquier medio o sistema de comunicación electrónica, la ley española debería

[119] Noticia publicada en el *Diario La Ley*, núm. 7826, de 27 de marzo de 2012.

igualmente incluir expresamente la posibilidad de grabar las conversaciones ambientales directas (las denominadas "vigilancias acústicas"), tanto en la vía pública, como en el domicilio u otros lugares cerrados, para acabar así con la controversia generada en torno a su licitud, a la vez que se equipararía con otros Ordenamientos europeos más avanzados (i. e., Alemania, Reino Unido e Italia) que prevén expresamente la posibilidad de utilizar dispositivos electrónicos para lograr la captación y grabación de las conversaciones privadas que el sospechoso mantenga en dichos lugares. Igualmente debería señalarse expresamente que tales dispositivos podrían perseguir la obtención tanto de sonidos como de imágenes, y que podrían ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado, o bien ser portados por el agente infiltrado, siempre con el correspondiente control judicial, dada la injerencia que tales medidas pueden ocasionar en los derechos de los sujetos investigados.

Por ello, estimamos insuficiente la propuesta de Código Procesal Penal (arts. 320 y ss), que permite la grabación de conversaciones (sonidos) en espacios abiertos públicos, así como en espacios cerrados y domicilios, mientras que sólo permite la captación de imágenes de espacios cerrados y domicilios cuando se refiera a la grabación de conversaciones entre el agente encubierto y los sujetos investigados. Esta limitación impedirá en la práctica, por ejemplo, el uso de cámaras de visión térmica para conocer desde el exterior si existe en el interior de un domicilio un peligro real para la vida (v. gr., un rehén en peligro de muerte, explosivos para evitar el asalto policial, etc).

5.

La futura reforma procesal debería diferenciar expresamente entre medidas de investigación referidas al registro de equipos informáticos, medidas referidas a la aprehensión de los datos almacenados en aquéllos, y medidas relativas a la intervención de los datos transmitidos, de acuerdo con las Recomendaciones europeas.

Además de prever legalmente el registro de tales dispositivos y la incautación de su contenido en términos que aseguren su integridad y autenticidad, debería permitir expresamente la posibilidad de extender el registro de un equipo informático a otros sistemas que se encuentren conectados al equipo originariamente investigado, cuando existan indicios de localizar en esos otros sistemas información relevante para la causa, pero siempre de conformidad con los Tratados y Convenios internacionales cuando tal ampliación en la búsqueda tenga efectos extraterritoriales o transfronterizos que excedan del ámbito de la jurisdicción española.

Igualmente, la ley deberá permitir tanto los registros *in situ* como los denominados "registros remotos" (registros *online*) sobre la información almacenada en un dispositivo electrónico, que permitan a las autoridades responsables de la investigación acceder de manera remota a un equipo o dispositivo, escanear su disco duro y demás unidades de almacenamiento, y remitir de una manera remota y automatizada toda esa información a otro equipo informático (el de la autoridad responsable de la investigación) en condiciones que aseguren su integridad y autenticidad.

6.

Debe preverse en la legislación procesal, y extrapolarse a otros dispositivos electrónicos susceptibles de almacenar ingentes cantidades de información personal, la doctrina recogida en la STC 173/2011, según la cual "el cúmulo de la información que se almacena por su titular en un ordenador personal (…) puede afectar al núcleo más profundo de su intimidad" y por lo tanto cualquier injerencia en el contenido de un ordenador personal deberá venir legitimada en principio por el consentimiento de su titular, o bien por una previa resolución judicial, salvo en los casos en los que se estime necesaria y urgente la actuación policial, por ejemplo, porque dicha actuación se desarrolle en el marco de la comisión de un delito flagrante, o exista un riesgo concreto e inminente para la vida de las personas como consecuencia de la utilización de tales dispositivos electrónicos (v. gr., la activación de una carga explosiva o la diseminación de un virus que dañe sistemas críticos para la seguridad nacional).

El acceso a esa extraordinaria cantidad y diversidad de información almacenable en los actuales dispositivos electrónicos que una persona puede llevar consigo (por ej., en la memoria de su smartphone o en un dispositivo USB) no puede ser considerado como una injerencia "leve" en la esfera de la privacidad de las personas, equiparable al examen de cartas, papeles, agendas o mochilas. Como bien ha reconocido el Tribunal Constitucional, "la versatilidad tecnológica que han alcanzado los teléfonos móviles convierte a estos terminales en herramientas indispensables en la vida cotidiana con múltiples funciones, (…) susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo al derecho al secreto de las comunicaciones (art. 18.3 CE), sino también a los derechos al honor, a la intimidad personal y a la propia imagen (art. 18.1 CE), e incluso al derecho a la protección de datos personales (art. 18.4 CE), lo que implica que el parámetro de control a proyectar sobre la conducta de acceso a dicho instrumento deba ser especialmente riguroso, tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la ley, como desde la perspectiva de si la concreta actuación desarrollada al amparo de la ley se ha ejecutado respetando escrupulosamente el principio de proporcionalidad".

Por ello, hay que celebrar positivamente y esperar que la futura reforma procesal mantenga lo dispuesto en el artículo 348 de la propuesta de CPP, según el cual será necesaria autorización judicial para proceder al registro de dispositivos de almacenamiento masivo de información, en consonancia con lo que ya pretendía regular el Anteproyecto de Ley de Enjuiciamiento Criminal de 2011.

El acceso a esa extraordinaria cantidad y diversidad de información almacenable en los actuales dispositivos electrónicos que una persona puede llevar consigo (por ej., en la memoria de su *smartphone* o en un dispositivo USB) no puede ser considerado como una injerencia "leve" en la esfera de la privacidad de las personas, equiparable al examen de cartas, papeles, agendas o mochilas. Por ello, hay que celebrar positivamente y esperar que la futura reforma procesal mantenga lo dispuesto en el proyectado art. 348 CPP, según el cual será necesaria autorización judicial para proceder al registro de dispositivos de almacenamiento masivo de información (arts. 347 y ss. CPP), en consonancia con lo que ya pretendía regular el Anteproyecto de Ley de Enjuiciamiento Criminal de 2011.

7.

Debe concretarse legalmente qué se entiende por «delito grave» a los efectos de permitir en el proceso penal medidas de investigación limitativas de derechos fundamentales, y en especial, cuando se trate del empleo de medidas tecnológicas de investigación (interceptación de telecomunicaciones, obtención de datos electrónicos, uso de dispositivos electrónicos para la captación de conversaciones e imágenes, así como para realizar labores de seguimiento y localización, registros de equipos informáticos y dispositivos electrónicos, etc.), pues la amplitud y heterogeneidad de los criterios judicialmente utilizados para definir qué se entiende por "delito grave" ha desbordado por completo la noción de delito grave establecida en el Código Penal.

Desde nuestro punto de vista, aunque el establecimiento de un listado de delitos o un umbral penológico a partir del cual puedan utilizarse determinadas medidas de investigación limitativas de Derechos Fundamentales puede resultar una opción plausible desde la óptica de la seguridad jurídica, resulta conveniente otorgar cierto margen para que para que las autoridades puedan valorar la proporcionalidad de su empleo conforme a las circunstancias concretas de cada caso –como, por ejemplo, que para su ejecución se hubieran empleado las TIC, o que se trate de delitos cometidos en el seno de una organización criminal–, pero siempre desde el prisma de una interpretación restrictiva de los supuestos en los cuales se admita la injerencia sobre los derechos fundamentales de las personas, que deben estar presididos por el principio de excepcionalidad y no constituir una regla general en la investigación de cualesquiera conductas delictivas.

La actual propuesta de reforma de nuestra vetusta LECrim coincide parcialmente con el anterior Anteproyecto del año 2011, en el sentido de concretar la gravedad del delito necesaria para legitimar la utilización de diversas medidas de investigación limitativas del Derecho al secreto de las comunicaciones, no sólo en función de un quantum punitivo asociado al delito objeto de la investigación, sino también en función de otros factores, como que se trate de delitos cometidos en el seno de la delincuencia organizada o a través de instrumentos y herramientas referidas a las nuevas tecnologías. No obstante, la pena a partir de la cual se legitimaría estas medidas de investigación se reduce desde los 5 años que preveía el art. 275 del anterior Anteproyecto de 2011, a los 3 años conforme con el propuesto artículo 295 CPP, lo cual no coincide con la noción de delito grave actualmente prevista en el Código Penal. Y además, resulta que esos presupuestos establecidos en el art. 295 de la propuesta de CPP serían aplicables a la intervención de las comunicaciones –tanto electrónicas como postales o telegráficas-, la grabación de conversaciones ambientales, la obtención de los datos asociados a una dirección IP o las numeraciones IMSI e IMEI de determinados aparatos de telefonía móvil, pero nada se concreta respecto de qué hechos delictivos podrían legitimar el uso de dispositivos de seguimiento y localización, un registro domiciliario, o el registro de dispositivos electrónicos. Es más, el registro remoto de equipos informáticos se prevé para una nueva modalidad: los "delitos de especial gravedad", que entendemos deberían concretarse por Ley en vez de esperar a que sea la jurisprudencia la que, con el tiempo, delimite esa especial gravedad del mismo modo que durante décadas ha precisado lo que entendía por trascendencia social.

8.

Por último, y en tanto no se produzca dicha concreción legal, tanto el Tribunal Constitucional como el Tribunal Supremo deberían proceder a corregir lo antes posible la actual interpretación de la Ley 25/2007 llevada a cabo por diversas Audiencias Provinciales[120], que estiman que la cesión a las autoridades de determinados datos referidos a comunicaciones electrónicas y conservados por las operadoras de telecomunicaciones, con motivo de una orden judicial, sólo pueden ser cedidos cuando se está investigando un delito grave contemplado en el Código Penal o en alguna ley penal especial conforme a lo dispuesto en el art. 13 CP, esto es, infracciones que la Ley castiga, entre otras, con penas de prisión superiores a 5 años o privaciones de derechos por igual o más tiempo.
La potencial lesividad del uso de instrumentos informáticos o electrónicos para la comisión de los delitos, así como la grave dificultad de su persecución por los medios tradicionales de investigación, son criterios que deben ponderarse necesariamente por el órgano judicial a la hora de permitir la utilización de ciertos medios especiales de investigación, incluso en aquellos supuestos en los que el delito pudiera llevar aparejada una pena "no grave", ya que puede resultar que tales medidas tecnológicas de investigación resulten las únicas idóneas para obtener datos relevantes para el descubrimiento o la comprobación del hecho investigado o para la identificación de su autor material, que no podrían obtenerse mediante otro medio de investigación menos gravoso.

En efecto, para la investigación de unas amenazas efectuadas a través de las Redes sociales, la identificación del titular desde cuya IP se efectuaron tales manifestaciones exigirá la solicitud de determinados datos a las operadoras de telecomunicaciones y prestadoras de servicios de Internet, pues será una medida trascendental y necesaria para la localización del autor de los hechos, aun cuando dicha conducta no esté castigada con una "pena grave". Y lo mismo podría decirse del delito de *hacking* (art. 197.3 CP), del delito de daños informáticos (art. 264 CP), o del delito de estafa informática del art. 248.2 CP (en sus múltiples modalidades comisivas como *phising, smishing, pharming,* etc.), cuyas penas no son "graves", y sin embargo, su investigación necesitará contar ineludiblemente con determinada información sobre las comunicaciones electrónicas efectuadas al tiempo de cometerse los hechos y almacenadas por las operadoras de telecomunicaciones. Como bien apuntó el citado Auto de la AP de Valencia, secc. 6ª, de 7 de junio de 2011, "la última modificación del Código Penal, introduce nuevos delitos realizados a través de Internet como el regulado en el art. 183 bis llamado ciberacoso, que está penado con pena entre 1 y 3 años de prisión o multa, que por sus penas podría entenderse como delito menos grave, pero que no tiene otra forma de investigarse que a través de la averiguación de las direcciones IP de los ordenadores desde donde se produjeron las comunicaciones".

Además, y de mantenerse la interpretación literal del art. 1.1 LCDCE, se daría la paradoja de que las autoridades judiciales no podrían solicitar la *cesión* de determinados datos conservados en poder de las operadoras con respecto a comunicaciones ya producidas y, sin embargo, sí podrían ordenar su *interceptación* en tiempo real en virtud

[120] Vid. AAP de Soria, secc. 1ª, núm. 164/2011, de 7 de noviembre de 2011; y AAP de Barcelona, secc. 3ª, de 26 de marzo (núm. 362/2012) y de 28 de septiembre (núm. 909/2012) de 2012.

de lo establecido en el art. 33 LGT. Para aumentar el contrasentido, la criticada interpretación del art. 1.1 LCDCE significaría exigir mayores requisitos para la cesión de datos externos a la comunicación que para el acceso al contenido de aquélla, a pesar de que tanto el Tribunal Constitucional como el Tribunal Supremo consideran que el conocimiento y uso de los datos de tráfico supone una «injerencia de menor intensidad[121]» en el Derecho al Secreto de las Comunicaciones del art. 18.3 CE que el conocimiento del contenido de las mismas.

[121] Vid. SSTC 123/2002 y 26/2006: *aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las «escuchas telefónicas», siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad*. Por su parte, la STS núm. 737/2009, de 6 de julio, ha llegado al extremo de defender que «esa menor intensidad debe proyectarse en un doble campo: en relación a la petición policial la entidad de los datos justificativos de la petición pueden ser menos intensos, y en relación a la autorización judicial, ésta puede serlo por providencia que, como se sabe no exige una motivación específica, bastando la remisión al oficio».

Bibliografía

AA.VV., The Symantec Internet Security Threat Report 2011 (the Norton Cybercrime Report), http://www.symantec.com/about/news/release/articl.jsp?prid=20110907_02.

ADLER, A. (2007): *The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act*, University of Miami Law Review, January, vol. 61.

ANDRÉS IBÁÑEZ, P. (1992): "Notas sobre la entrada y registro y la intervención telefónica", Planes Provinciales y Territoriales de Formación, vol. II, CGPJ.

BELLIA, P. L. (2011): *Chasing Bits across Borders*, The University of Chicago Legal Forum.

BELLIA, P. (2004): "The future of internet surveillance", The George Washington Law Review, August, 72.

BRENNER, S. / KOOPS, B. J. (2004): "Approaches to Cybercrime Jurisdiction", Journal of High Technology Law, Vol. IV No. 1.

BRENNER, S. W. / SCHWERHA IV, J. J. (2008): "Cybercrime Havens. Challenges and Solutions", *Business Law Today*, vol. 17, nov-dec.

BRENNER, S. (2007): "At light speed: attribution and response to cybercrime/terrorism/Warfare", *Journal of Criminal Law & Criminology*, nº 97.

CABEZUDO BAJO, M. J. (2004): "La inviolabilidad del domicilio y el proceso penal", ed. Iustel, Madrid, p. 71 y ss.

CASEY, E. (2004): *Digital Evidence and Computer Crime*, 2nd Edition, ed. Elsevier, London.

CRESPO BARQUERO, P. (2010): "Intervenciones judiciales en materia de comunicaciones telefónicas e Internet", *Cuadernos Penales José María Lidón*, núm.7.

CSONKA; P. (2006): "The Council of Europe´s Convention on Cyber-Crime and other european initiatives", *Revue Internationale de Droit Pénal*, vol. 77.

DE HERT, P. (2006): "Cybercrime and Jurisdiction in Belgium and the Netherlands…", en KOOPS, B .J. / BRENNER, S. W., *Cybercrime and Jurisdiction. A Global Survey*, ed. T.C.M. Asser Press, The Hague.

DEL MORAL GARCÍA, M.: "La intervención de las comunicaciones en centros penitenciarios", La Ley, núm. 7573, de 21 de febrero de 2011.

DÍAZ CABIALE, J. A. (1991): *La admisión y práctica de la prueba en el proceso penal*, ed. CGPJ, Madrid.

DÍAZ REVORIO, F. J. (2008): "La constitución ante los avances científicos y tecnológicos: breves reflexiones al hilo de los recientes desarrollos en materia genética y en tecnologías de la información y la comunicación", *Revista de Derecho Político de la UNED*, nº 71-72.

FÁBREGA RUIZ, C. (1997): "Secreto de las comunicaciones y proceso penal", La Ley, 1997-4.

FREIWALD, S. (2004): "Online Surveillance: Remembering the Lessons of the Wiretap Act", Alabama Law Review, Fall, 56.

GALÁN MUÑOZ, A. (2009): "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", *Revista Penal*, nº24, julio 2009.

GARCÍA RUIZ, J. M.(2003): "Correo electrónico y proceso penal", La Ley nº5805, de 18 de junio de 2003.

GERCKE, M. (2009): Understanding cybercrime: a Guide for Developing Countries, 2009. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

GIMENO SENDRA, V.(2009): "La intervención de las comunicaciones", La Ley, núm. 7192, de 9 de junio de 2009.

GOLDSCHMITH, J. (2001): "The Internet and the Legitimacy of Remote Cross-Border Searches", Public Law and Legal Theory Working Paper no. 16, 2001.

GOLDSMITH, J. L. (1999): "Cybercrime and Jurisdiction". Presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California, Dec. 6-7.

GONZÁLEZ TAPIA, M. I. (2002): "El concepto de delito a distancia", en VV.AA. (Coordinador: Juan José GONZÁLEZ RUS), El Código Penal de 1995, cinco años después, ed. Servicio de Publicaciones de la Universidad de Córdoba, Córdoba.

GONZÁLEZ-CUÉLLAR SERRANO, N. (2006): "Garantías constitucionales en la persecución penal en el entorno digital", en VV.AA., Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García, ed. Colex, Madrid.

HERNÁNDEZ GUERRERO / ÁLVAREZ DE LOS RÍOS, (1999) "Medios informáticos y proceso penal", Estudios Jurídicos. Ministerio Fiscal, 1999-IV, p. 497.

JACOBY, N. (2007): "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States", *Georgia Journal of International and Comparative Law*, vol. 35, nº3.

JIMÉMEZ CAMPO, J. (1987): "La garantía constitucional del secreto de las comunicaciones", *Revista Española de Derecho Constitucional*, nº20.

KERR, O. (2005): "Digital Evidence and the new Criminal Procedure", Columbia Law Review, vol. 105, pp. 279 y ss.

KERR, O. (2006): "Search and Seizure in a Digital World", Harvard Law Review, vol. 119, (disponible en: http://ssrn.com/abstract=697542).

LLAMAS FERNÁNDEZ, M. / GORDILLO LUQUE, J. M. (2007): "Medios técnicos de vigilancia", en VV.AA.: *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, 2007-II, CGPJ.

LÓPEZ BARJA DE QUIROGA, J. (1989): Las escuchas telefónicas y la prueba ilegalmente obtenida, ed. Akal, Madrid, 1989.

MACK, M. (2000): "Electronic Discovery vs. Computer Forensics", New Jersey Law Journal. Vol. 20, October 2000.

MARCHENA GÓMEZ, M. (2006): "Dimensión jurídico penal del correo electrónico", *La Ley,* 4 de mayo de 2006.

MARCHENA GÓMEZ, M. (2011):, "La vulneración de derechos fundamentales por ministerio de la Ley (a propósito del art. 33 de la Ley General de Telecomunicaciones)", La Ley, núm. 7572, de 18 de febrero de 2011.

MORENO CATENA, V. (1997), "La intervención de las comunicaciones personales en el proceso penal", VV.AA., *La reforma de la Justicia penal: estudios en homenaje al Prof. Klaus Tiedemann*, Servicio de Publicaciones de la Universidad Jaume I, Castellón.

MUÑOZ DE MORALES ROMERO, M. (2005): "Hacia la cobertura legal de las intervenciones telefónicas en el ordenamiento jurídico español: La reforma del art. 579 LECrim", Boletín de la Facultad de Derecho de la UNED, nº 27.

NIEVA FENOLL, J. (2005) "Las pulseras telemáticas: aplicación de las nuevas tecnologías a las medidas cautelares y a la ejecución en el proceso penal", *Revista del poder judicial*, núm. 77.

NOYA FERREIRO, M. L. (2000), *La intervención de las comunicaciones orales directas en el proceso penal,* ed. Tirant lo Blanch, Valencia.

RAFOLS LLACH, J. (1992), "Autorización judicial para la instalación de aparatos de escucha, transmisión y grabación en lugar cerrado", *Cuadernos de Derecho Judicial*, CGPJ, Madrid, vol. I.

RIVES SEVA, A. P. (2010) *La intervención de las comunicaciones en el proceso penal. Análisis doctrinal, legislación y jurisprudencia*. Ed. Bosch, Barcelona.

RODRÍGUEZ LÁINZ, J. L. (2010): "De vueltas con SITEL", La Ley, núm. 7515, de 23 de noviembre de 2010.

RODRÍGUEZ LAINZ, J. L. (2012), "Hacia un nuevo entendimiento del concepto de gravedad del delito en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas", *Diario La Ley*, nº7789, de 2 de febrero de 2012.

SÁNCHEZ NÚÑEZ, T. (2007): "Jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal", en VV.AA., Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia, *Cuadernos de Derecho Judicial*, 2007-II, CGPJ.

SEITZ, N. (2004): "Transborder Search: A New Perspective in Law Enforcement", Yale Law School, http://www.yjolt.org/files/seitz-7-YJOLT-23.pdf.

SHELTON, D. E. (2008), "The 'CSI Effect': Does It Really Exist?", *NIJ Journal*, Issue No. 259.

SHELTON, D.E., KIM, Y.S., BARAK, G. (2006): "A Study of Juror Expectations and Demands Concerning Scientific Evidence: Does the 'CSI Effect' Exist?," *Vanderbilt Journal of Entertainment and Technology Law*, vol. 9, nº2.

TORRES MORATO, M. A. (con DE URBANO CASTRILLO, E.) (1997) *La prueba ilícita penal: estudio jurisprudencial*, Editorial Aranzadi.

URBANO DE CASTRILLO, E. (2007), "La investigación tecnológica del delito", en VV.AA.: Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia, *Cuadernos de Derecho Judicial*, 2007-II, CGPJ.

VELASCO NÚÑEZ, E. (2011), "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal", *La Ley Penal*, núm. 82.

VELASCO NÚÑEZ, E. (2007): "Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos", en VV.AA., *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, 2007-II, CGPJ.

VELASCO NÚÑEZ, E. (2010): *Delitos cometidos a través de Internet. Cuestiones Procesales,* ed. La Ley, Madrid, 2010.

Trabajos publicados

EP 1/1999	Cuadernos con alternativas 1. Varios autores.
EP 2/1999	Cuadernos con alternativas 2. Varios autores.
EP 3/1999	Bases para una reforma de la política. Varios autores.
EP 4/2000	La educación a debate. Victoria Camps.
EP 5/2000	Un pacto de Estado para la justicia. Varios autores.
EP 6/2000	Sistema Nacional de Salud. Javier Rey.
EP 7/2001	La Universidad Europea del Trabajo. Varios autores.
EP 8/2001	La judicialización en la Unión Europea. Quién gana y quién pierde. Antonio Estella.
EP 8 bis/2001	La liberalización de los servicios de interés económico general. Un modelo progresista dentro y para Europa. Leonor Moral.
EP 9/2002	La armonización del impuesto sobre la renta de las personas físicas en el marco del debate federalista. Posibilidades y límites. Violeta Ruiz.
EP 10/2002	La participación de los españoles en elecciones y protestas. Belén Barreiro.
EP 11/2002	La Constitución europea y la Carta de Derechos fundamentales. María Luisa Fernández.
EP 11 bis/2003	El proceso constituyente europeo en sentido estricto. Relanzar la integración desde la ciudadanía. Rosa Velázquez.
EP 12/2003	Las nuevas formas de participación en los gobiernos locales. Eloísa del Pino y César Colino.
EP 13/2003	El proceso de globalización. Análisis de las propuestas alternativas al Consenso de Washington. Carlos Garcimarín y Santiago Díaz de Sarralde.
EP 14/2004	El modelo social en la Constitución europea. José Vida.
EP 15/2004	Los procesos migratorios. Alternativas al discurso dominante. Arantxa Zaguirre.
EP 16/2005	La enseñanza de la religión católica en España. Margarita Lema.
EP 17/2005	Ciudadanía y minorías sexuales. La regulación del matrimonio homosexual en España. Kerman Calvo.
EP 18/2005	La financiación de las confesiones religiosas en España. Alejandro Torres.
EP 19/2006	Propuestas para la reforma del sistema electoral español. Rubén Ruiz.
EP 20/2006	Mujer y vivienda. Una aproximación al problema de la vivienda desde una perspectiva de género. Jordi Bosch.
EP 21/2006	La restricción de derechos fundamentales en el marco de la lucha contra el terrorismo. M.ª Ángeles Catalina Benavente.
EP 22/2006	Una propuesta para la enseñanza de la ciudad democrática en España. Irene Martín Cortes.
EP 23/2006	Los símbolos y la memoria del Franquismo. Jesús de Andrés Sanz.
EP 24/2007	Cambios en las relaciones de trabajo y derecho a la huelga. Xavier Solà Monells y Daniel Martínez Fons.
EP 25/2007	Modelos familiares y empleo de la mujer en el Estado de bienestar español. Almudena Moreno Mínguez.
EP 26/2007	La exclusión social: análisis y propuestas para su prevención. Anabel Moriña Díez.

EP 27/2007	La reforma del Senado. Alberto Penadés e Ignacio Urquizu-Sancho.
EP 28/2007	Un nuevo enfoque de la solidaridad autonóma a través de los Fondos de Compensación Interterritorial. Roberto Fernández Llera y Francisco J. Delgado Rivero.
EP 29/2007	Derecho de asilo y mutilación genital femenina: mucho más que una cuestión de género. Yolanda García Ruiz.
EP 30/2008	El desarrollo de políticas públicas locales como garantes de la satisfacción de los ciudadanos. Pablo Gutiérrez Rodríguez y Marta Jorge García-Inés.
EP 31/2008	El turismo residencial y las políticas públicas europeas. Fernando J. Garrigós Simón y Daniel Palacios Marqués.
EP 32/2008	La economía social y su participación en el desarrollo rural. Andrés Montero Aparicio.
EP 33/2008	Prostitución y políticas públicas: entre la reglamentación, la legalización y la abolición. Pedro Brufao Curiel.
EP 34/2008	La dimensión territorial de la pobreza y la privación en España. Jesús Pérez Mayo.
EP 35/2008	"Ampliar para ganar": las consecuencias electorales del crecimiento del Metro en Madrid, 1995-2007. Luis de la Calle Robles y Lluís Orriols i Galve.
EP 36/2008	Las causas de la participación y sus consecuencias en el voto de centro y de izquierda en España. Sebastián Lavezzolo Pérez y Pedro Riera Segrera.
EP 37/2008	El medio ambiente urbano en la Unión Europea. Susana Borràs Pentinat.
EP 38/2008	Control político y participación en democracia: los presupuestos participativos. Ernesto Ganuza Fernández y Braulio Gómez Fortes.
EP 39/2008	Cataluña después del primer "Tripartit". Continuidad y cambio en patrones de comportamiento electoral. Laia Balcells Ventura y Elna Roig Madorran.
EP 40/2009	La reducción de empleo y sus consecuencias en los resultados: un análisis de las empresas españolas. Fernando Muñoz Bullón y María José Sánchez Bueno.
EP 41/2009	Flexicurity and Gender Equality: advancing flexicarity policies in Denmark and Spain. Óscar García Agustín y Lise Rolandsen Agustín.
EP 42/2009	La cobertura de la situación de dependencia. Djamil Tony Kahale Carrillo.
EP 43/2009	Políticas públicas y segregación residencial de la población extranjera en la Comunidad de Madrid. Alfonso Echazarra de Gregorio.
EP 44/2009	Libre circulación de personas y ciudadanía social: ¿cabe imponer barreras al turismo social?. Borja Suárez Corujo y Tomás de la Quadra-Salcedo Janini.
EP 45/2009	Nuevos desafíos democráticos: hacia una iniciativa legislativa popular efectiva. Carmela Mallaina García.
EP 46/2009	La deconstrucción del servicio público de televisión: hacia una política de innovación en las nuevas plataformas digitales. Alberto González Pascual.
EP 47/2010	Desigualdad de rentas y desigualdad de oportunidades en España. Christelle Sapata.

EP 48/2010	Un análisis del efecto de la Ley de igualdad en la representación electoral, parlamentaria y en el comportamiento electoral de las mujeres en las elecciones generales de 2008. Álvaro Martínez Pérez y Kerman Calvo Borobia.
EP 49/2010	¿Querer es poder? Un análisis de la fecundidad de las mujeres españolas e inmigrantes. María José Hierro Hernández y Margarita Torre Fernández.
EP 50/2010	Salud y acceso a los servicios sanitarios en España: la realidad de la inmigración. Cristina Hernández Quevedo y Dolores Jiménez Rubio.
EP 51/2010	Las políticas de conciliación en España y sus efectos: un análisis de las desigualdades de género en el trabajo del hogar y el empleo. Pablo Gracia y Daniela Bellani.
EP 52/2010	¿Debe el agua de los ríos llegar al mar? Orientaciones para una gestión medioambiental del agua en España. Fernando Magdaleno Mas.
EP 53/2010	The Internet Sector and Network Neutrality: where does the EU stand? Hairong Mu y Carlo Reggiani.
EP 54/2010	Políticas migratorias comparadas en el Sur de Europa: lecciones cruzadas entre España y Portugal. Belén Fernández Suárez.
EP 55/2010	Los biocombustibles en la política energética europea: los retos de la estrategia energética europea para el año 2020. Raquel Montes Torralba.
EP 56/2010	Blogging político y personalización de la democracia local en España y Portugal. Evidencias presentes y propuestas de futuro. J. Ignacio Criado y Guadalupe Martínez Fuentes.
EP 57/2010	Democracia participativa, sociedad civil y espacio público en la Unión Europea. Luis Bouza García.
EP 58/2011	La imposición sobre el patrimonio como instrumento para una distribución equitativa de la riqueza. César Martínez
EP 59/2011	Políticas migratorias comparadas en el Sur de Europa: lecciones cruzadas entre España y Portugal. Belén Fernández Suárez.
EP 60/2011	Los biocombustibles en la política energética europea: los retos de la estrategia energética europea para el año 2020. Raquel Montes Torralba.
EP 61/2011	Reformas institucionales de la gobernanza económica internacional en tiempos de cambio: debate de ideas, instituciones y política económica. Gonzalo Caballero
EP 62/2011	Nuevas herramientas. Nuevas ideas. Utilización de campañas de base en España. Elecciones regionales y locales en 2011. Bernardo Navazo López.
EP 63/2011	Un estudio en torno a la edad de jubilación. Sonia Fernández Sánchez.
EP 64/2011	El derecho a una vivienda adecuada. Un derecho del siglo XXI. Vanessa Villalibre.
EP 65/2011	Las políticas de revitalización urbana en ciudades intermedias de tradición minero-industrial: incidencia de los actores locales. José Prada Trigo.
EP 66/2011	Articulación entre las relaciones familiares y sociales y la discapacidad en Europa. Laura Lorenzo Carrascosa.
EP 67/2011	Calidad y reforma de la Educación Secundaria Obligatoria en España.

	Flor Arias y Alessandro Gentile.
EP 68/2011	Propuesta de reforma del sector hipotecario español: análisis de la oportunidad de la dación en pago. Tomás Gimeno.
EP 69/2012	"Guardar al defensor de la Constitución". Sobre la independencia de la jurisdicción constitucional: evaluación de alternativas institucionales. Pablo José Castillo Ortiz
EP 70/2012	Análisis y propuestas de actuación ante la reforma de la Política Pesquera Común. La sostenibilidad como eje de futuro de la pesca española. Miquel Ortega Cerdá
EP 71/2012	El régimen de garantía de ingresos mínimos en España: una propuesta de revisión. Borja Barragué Calvo y César Martínez Sánchez
EP 72/2013	Políticas urbanas innovadoras, gobernanza y planificación flexible: análisis de la evolución en Francia y propuestas de adaptación al contexto español. Beatriz Fernández Águeda
EP 73/2013	Emancipación juvenil en tiempos de crisis: Un diagnóstico para impulsar la inserción laboral y la transición residencial. Alessandro Gentile