BOLETÍN DEL MINISTERIO DE JUSTICIA

Año LXXI | Núm. 2.195 | Enero de 2017

GOBIERNO DE ESPAÑA
MINISTERIO DE JUSTICIA

ISSN: 1989-4767
NIPO: 051-15-001-5
www.mjusticia.es/bmj

Enlaces

Publicaciones del Ministerio de Justicia

Catálogo de publicaciones de la Administración General del Estado. https://cpage.mpr.gob.es

Contacto

Contacto Boletín

Edita
Ministerio de Justicia
Secretaría General Técnica

Maquetación
Subdirección General de Documentación y Publicaciones

ISSN
1989-4767

NIPO
051-15-001-5

Depósito Legal
M.883-1958

SUMARIO

AÑO LXXI • Enero 2017 • Núm. 2.195

SECCIÓN DOCTRINAL

Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015

LORENA BACHMAIER WINTER[1]

Resumen:

Este estudio analiza el marco legal previsto por la reforma de la LO 13/2015 para el registro remoto de equipos informáticos a través de la instalación de software, con el fin de valorar si esa regulación logra alcanzar el difícil equilibrio entre los intereses en juego en todo proceso penal. Se persigue también mostrar que los criterios utilizados hasta ahora para valorar la proporcionalidad de los registros de objetos tangibles, o las escuchas telefónicas, puede que no sean adecuados en relación con una medida tan invasiva como es el registro remoto de equipos informáticos.

Abstract:

This study analyses the provisions on the search of computers with the help of forensic software introduced by the LO 13/2015 in order to check if this legal reform has struck the right balance between the public interest in prosecuting crimes committed through the use of information and communications technologies and the respect for the citizens' right to privacy. It will be argued that the criteria applied until now for assessing the proportionality and need of searches regarding tangible things, might have to be revisited in the case of searches of computers.

Palabras clave:

investigación penal, prueba, registro e incautación, medidas investigación telemáticas, derechos fundamentales, proporcionalidad.

Keywords:

criminal investigation, digital evidence, search and seizure, electronic surveillance, fundamental rights, proportionality.

---

[1] Catedrática de Derecho Procesal, Universidad Complutense de Madrid.

Fecha de recepción: 9-11-2016. Fecha de aceptación: 12-12-2016

1. Introducción

Tras largos años reclamando la reforma de la Ley de Enjuiciamiento Criminal en materia de interceptación de las telecomunicaciones y otras medidas de investigación tecnológica, la Ley Orgánica 13/2015 aborda la regulación de estas medidas de manera decidida y con la amplitud necesaria[2]. La reforma abarca medidas de investigación muy diversas: la interceptación de las comunicaciones (telefónicas, telemáticas o comunicaciones orales directas); el acceso a datos electrónicos ya almacenados (de contenido, de tráfico o asociados); el registro de equipos informáticos, tanto directamente, como a través de un ordenador en red o del acceso remoto mediante la instalación de s*pyware*[3]; las operaciones mediante agente encubierto en la red; la utilización de dispositivos de seguimiento; o la captación y grabación clandestina de imágenes tanto en espacios públicos como privados. Además, la reforma contempla medidas de protección de datos, así como las obligaciones de cooperación de los proveedores de servicios de telecomunicaciones en la investigación criminal.

En lo que se refiere a las medidas de investigación tecnológica, como puede observarse, el alcance de esta reforma es bastante amplio. En este trabajo no pretendo realizar un análisis de todas esas medidas, sino que me centraré únicamente en una de las más novedosas: el registro remoto de equipos informáticos. Se trata de una medida muy invasiva en la esfera de los derechos fundamentales y que no deja de plantear serios problemas en cuanto a su alcance transnacional. Antes de analizar la regulación introducida por el legislador español, conviene aclarar, aunque sea muy brevemente, algunos términos.

---

[2] *Ley Orgánica 13/2015*, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Sobre el contenido de esta Ley, en general *vid.* MARCHENA GÓMEZ, M., y GONZÁLEZ-CUÉLLAR, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid 2015, sobre las medidas de investigación tecnológica, en particular, pp. 173 y ss. Sobre las medidas de investigación en concreto, desde un enfoque de la teoría constitucional *vid.* ZOCO ZABALA, C., *Nuevas tecnologías y control de las comunicaciones,* Madrid 2015. *Vid.* también, aunque sin referirse al registro remoto de ordenadores, BUENO DE MATA, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», *La Ley,* n.º 8627, 19 octubre 2015; JIMÉNEZ SEGADO, C., y PUCHOL AIGUABELLA, M., «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos», *La Ley*, n.º 8676, 7 enero 2016, pp. 1-10; GARCÍA SAN MARTÍN, J., «Consideraciones en torno al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», *La Ley*, n.º 8468, 28 enero 2015; DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», *La Ley*, n.º 8693, 2 febrero 2016, pp. 1-14; RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», La Ley, n.º 8808, 21 julio 2016, pp.1-15.

[3] A lo largo de este trabajo se utilizan con frecuencia los términos en inglés, pues su uso está aceptado y extendido en el ámbito de la informática, y, por tanto, también en el ámbito jurídico que se ocupa de las medidas tecnológicas.

El acceso remoto a equipos informáticos puede llevarse a cabo fundamentalmente de dos maneras: 1) accediendo a los datos a través de una red *(computer network)* que sea accesible a través del equipo que se ha localizado e intervenido físicamente, bien sea como consecuencia de una entrada y registro o de otra manera; y 2) mediante el acceso a los datos almacenados en equipos informáticos que no están físicamente localizados o accesibles, pero a los cuales puede accederse mediante la utilización de programas espía o *spyware,* un software específico que permite «entrar» en el equipo, sin que, de ordinario, su usuario lo advierta. La primera medida suele denominarse registro ampliado o *extended search of computers,* y la segunda registro remoto o *remote search of computers*. Además, a través del registro remoto a través de *spyware,* se podría a su vez acceder a otros equipos que estuvieran conectados a la red del equipo «intervenido» o «hackeado». Estos supuestos requieren un análisis separado pues, aunque el acceso al equipo informático se produce en ambos casos a distancia o de modo remoto, la forma de acceso es diferente y su regulación también difiere en lo que se refiere a los presupuestos y a su ámbito de aplicación. En este trabajo solo me ocuparé del registro remoto de equipos informáticos a través de la instalación de *spyware*. El registro ampliado deriva bien del registro directo de un dispositivo de almacenamiento –que está conectado en red a otros equipos– o bien de un registro remoto a través de programas espía, por lo que siempre estará vinculado a alguna de esas dos medidas.

A continuación se analizará si el marco legal previsto por la reforma de la LO 13/2015 resulta adecuado, y si en esa regulación el legislador permite lograr el difícil equilibrio entre los intereses en juego: de un lado, el interés público en el esclarecimiento de los hechos delictivos, especialmente aquellos cometidos a través de internet y a través del uso de tecnologías de la información y la comunicación (en adelante TICs), y, de otro lado, la protección del derecho fundamental a la privacidad de los ciudadanos. Intentaré mostrar también que los criterios utilizados hasta ahora para valorar la proporcionalidad de los registros de bienes u objetos tangibles, o las interceptaciones telefónicas, no son adecuados para valorar la proporcionalidad de una medida tan invasiva como es el registro remoto de equipos informáticos.

2. Registro remoto de equipos informáticos

Además de regular el registro de equipos informáticos mediante su acceso físico, la Ley Orgánica 13/2015 introduce por primera vez en nuestro ordenamiento jurídico normas relativas al registro remoto de los mismos. Desde hace años, el Consejo de la Unión Europea lleva recordando a los Estados miembros la conveniencia de regular esta medida de investigación[4], aunque ha habido que esperar hasta octubre de 2015 para que España se hiciera eco de esas demandas. Su regulación figura en el presente art. 588 septies (a) LECRIM, precepto que regula sus presupuestos y ámbito de

[4] *Vid*. Consejo de la Unión Europea, *Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime*, 2987th Justice and Home Affairs Council meeting, 27-28 de noviembre de 2008, disponible en: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/104344.pdf.

aplicación[5], pero que ha de completarse con las normas generales sobre medidas de investigación tecnológicas. Esta medida es completamente novedosa en el ámbito del proceso penal español, pues hasta ahora no solo no estaba prevista legalmente, sino que tampoco estaba autorizada mediante una interpretación extensiva de las normas de la interceptación de las comunicaciones, ni de las normas sobre registro e incautación de documentos.

La instalación de *spyware* para acceder de manera remota a equipos informáticos es una medida que todavía resulta muy controvertida debido al grado de intromisión que implica en la esfera de privacidad de las personas[6]. A diferencia del registro domiciliario

---

[5] Registros remotos sobre equipos informáticos:

Artículo 588 septies (a) Presupuestos.

«1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.»

[6] En este trabajo se hace referencia en general al derecho a la privacidad, sin abordar las diferenciaciones del artículo 18 de la Constitución española: el término privacidad englobaría tanto el derecho fundamental al secreto de las comunicaciones del art. 18.3 como el derecho a la intimidad del art. 18.1 CE. Supera el ámbito de este trabajo analizar el diferente alcance y contenido de esos derechos constitucionales, además de que ya existe una abundante bibliografía al respecto. Por otro lado, a los efectos del análisis que aquí se realiza, es suficiente hacer referencia en general al derecho a la privacidad, tal y como se hace en el art. 8 del Convenio Europeo de Derechos Humanos. Sobre la afectación de los derechos del art. 18 de la Constitución española, y específicamente en relación con las medidas de investigación tecnológicas, me remito a ZOCO ZABALA, C., ob. cit.,

y del registro físico de un ordenador hallado durante la entrada en un domicilio o en otro lugar público, en el registro remoto el afectado no es conocedor del acceso a sus datos[7]. Este último aspecto hace del acceso clandestino al equipo informático de una persona una herramienta muy poderosa, pues no solo permite acceder a una ingente cantidad de datos y comunicaciones, sino que, además, puede extenderse en el tiempo, con lo que la intromisión en el derecho a la privacidad es especialmente importante[8].

Junto con Francia e Italia, España es uno de los pocos países de la Unión Europea que regula expresamente el registro remoto de equipos informáticos a través de la instalación de *software* espía como una medida de investigación criminal. Conforme a los datos del estudio llevado a cabo por el Instituto Max Planck de Derecho Penal de Friburgo, en materia de interceptación de las comunicaciones en la Unión Europea[9], en Alemania[10], como en la República Checa[11], la instalación de *software* no se regula expresamente en el ámbito del proceso penal, lo cual crea la incertidumbre acerca de si tal medida está autorizada o no. En Bélgica, Holanda y Suecia se permite acceder de forma remota a equipos informáticos *(remote surveillance)*[12], pero ello deberá

---

pp. 21 y ss.; VIDAL FUEYO M. C., «La constitucionalidad de determinadas diligencias de investigación policial que afectan a la intimidad» en *La Constitución política de España: Estudios homenaje a Manuel Aragón Reyes* (Rubio Llorente, Jiménez Campo, Solazábal Echevarría, Biglino Campos y Gómez Montoro, coords.), Madrid 2016, pp. 947-966.

[7] Un interesante análisis sobre los derechos fundamentales afectados a través de los registros *on-line* se llevó a cabo por el Tribunal Constitucional alemán en su sentencia de 27 de febrero de 2008, disponible en http://www.bundesverfassungsgericht.de,1 BvR 370/07,1 BvR 595/07. Sobre esta sentencia *vid.*, entre otros, BÖCKENFÖRDE, T., «Auf dem Weg zur elektronischen Privatsphäre», *Juristenzeitung*, 19/2008, pp. 925-939. *Vid*., también Abel, W., «Agents, trojans and tags: The next generation of investigators», 23 *International Rev. of Law Computers & Technology*, vol. 23 (March) 2009, pp. 99-108, p. 103.

[8] No comparto la afirmación de que el registro *on-line* «no es más que una modalidad en cuando al modo de acceder al contenido de un equipo informático», como sostiene ORTIZ PRADILLO, J.C., «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica», en J. Pérez Gil (ed.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, Madrid 2012, pp. 267-310, p. 308. Si bien es cierto que técnicamente solo se diferencia en el modo de acceder al ordenador, en cuanto a la lesividad del derecho, por razón de su clandestinidad, es mucho mayor.

[9] *Vid.* U. Sieber y N. von zur Mühlen (eds.), *Access to Telcommunication Data in Criminal Justice. A comparative Analysis of European Legal Orders,* Berlin 2016, en particular pp. 101-111. Deseo expresar mi agradecimiento a los redactores de este informe, U. Sieber, N.von zur Mühlen y T. Tropina, por compartir algunos de sus resultados sobre el registro remoto de equipos informáticos antes de su publicación oficial.

[10] *Vid.* B. VOGEL, P. KÖPPEN y T. WAHL, «Access to Telcommunication Data in Germany», en *Access to Telcommunication Data in Criminal Justice*, cit., pp. 551-563. *Vid.*, también, Böckenförde, T., ob. cit., pp. 933 ss.; BRAUN, F., «Ozapftis–(Un)Zulässigkeit von Staatstrojanern», *Kommunikation und Recht*, 11/2011, pp. 681-686.

[11] *Vid.* R. POLCAK, «Access to Telcommunication Data in the Czech Republic and Slovakia», en *Access to Telcommunication Data in Criminal Justice,* cit., pp. 395-401.

[12] T. TROPINA, «Comparative Analysis», en *Access to Telcommunication Data in Criminal Justice,* cit., pp. 100-111.

realizarse mediante la instalación física en el ordenador del s*oftware* que se precisa: no se permite instalar el *spyware* a través del acceso remoto, solo la vigilancia remota una vez que se instala directamente el programa espía. En el Reino Unido el registro remoto de equipos informáticos no es una medida novedosa, pues, a pesar de no estar regulada en el ámbito del proceso penal, sí se encuentra prevista desde hace tiempo en la normativa policial[13].

En los siguientes epígrafes se analizará el contenido del art. 588 septies (a) LECRIM, los presupuestos generales para la aplicación de esta medida, y el control judicial a través del auto autorizando el registro remoto de un ordenador y el acceso a sus datos.

3.1 Principio de especialidad y grado de sospecha de la comisión de un delito

El sistema español, a diferencia de otros ordenamientos, no permite utilizar medidas de investigación restrictivas de derechos fundamentales con fines preventivos o prospectivos[14]. En relación con las medidas de investigación tecnológicas, el art. 588 bis (a) (2) LECRIM lo prohíbe expresamente: «El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva».

Esto implica que toda medida de investigación tecnológica –y también el registro remoto de ordenadores– solo pueda acordarse si la medida se requiere para la investigación de un delito en particular. Así lo declaró expresamente el Tribunal Constitucional en su sentencia 253/2006, de 11 de septiembre: las medidas de investigación restrictivas del derecho a la privacidad (en aquel caso se trataba de unas escuchas telefónicas) solo son válidas si se autorizan sobre la base de indicios objetivos y concretos de un delito, y no sobre meras hipótesis o sospechas generales[15]. Con ello se persigue evitar que los instrumentos del proceso penal sean utilizados para llevar a cabo intervenciones prospectivas, o una *inquisitio generalis* de la vida de los ciudadanos con fines preventivos[16]. Lógicamente, el alcance del principio de

---

[13] *Vid*. ABEL, W., ob. cit., p. 101, quien afirma lo siguiente: «the method was quietly adopted in the UK when the relevant technology to remotely access computers became available and, according to the Association of Chief Police Officers, British police have been carrying out remote searches in the past and stated that 194 remote hacking operations were undertaken in 2007-2008» No obstante, la medida se utilizaba antes de su completa regulación en la legislación policial en RIPA in 2000 *(Regulation of Investigatory Powers Act)*. *Vid*. también, BRENNER, S.W., «Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force», *Mississippi Law Journal* 81-5 (2011-2012), pp. 1229-1261, p. 1236.

[14] A diferencia de Alemania, donde la medida de registro remoto de equipos informáticos se regula como medida en el ámbito de la seguridad o prevención de delitos, tanto en el ámbito de inteligencia *(Verfassungsschutz)* como por las fuerzas de seguridad *(Polizeirecht)*. Hasta este momento, sin embargo, no se regula como medida de investigación penal en su código procesal penal (StPO), *vid.* BÖCKENFÖRDE, T., ob. cit., pp. 932-933.

[15] En igual sentido, SSTC 197/2009 o 219/2009. *Vid*. también ZOCO ZABALA, C. ob. cit., pp. 210-211.

[16] Acerca de la prohibición de utilizar el proceso penal para llevar a cabo una *inquisito generalis vid*. el estudio monográfico de AGUILERA MORALES, M., *Proceso penal y causa general*, Madrid, 2008.

especialidad está directamente relacionado con el grado o intensidad de las sospechas que justificarían la adopción de la medida restrictiva[17].

Por tanto, las meras sospechas, conjeturas subjetivas o suposiciones no son suficientes para autorizar el registro de un equipo informático y menos aún su acceso remoto. Dicho esto, sin embargo, ni la doctrina ni la jurisprudencia, como ya se ha mencionado, establecen una diferenciación clara entre «sospechas razonables», «indicios racionales» y «delito probable» a la hora de medir el grado de sospecha. Por su parte, el requisito de «probable cause» que figura en la Cuarta Enmienda de la Constitución de los EE.UU. está referido a la probabilidad de encontrar pruebas del delito. Al solicitar autorización para un registro, los agentes han de acreditar «probable cause» de que van a encontrar pruebas de un delito, y deben además describir en detalle qué pruebas es probable que se hallen. Por supuesto, las pruebas se referirán a un delito específico, pero como tal la «probabilidad» exigida se refiere directamente a la prueba, y no a la probabilidad de que el delito se haya cometido, como sucede en el sistema procesal español.

Habrá que concluir que quizás no pueda trazarse una distinción clara entre estos conceptos, más allá de sostener que unos implican unos niveles de sospecha más intensos que otros. Por ello, los intentos de delimitar estos términos por parte de la jurisprudencia incluyen también conceptos indefinidos, tales como la referencia a «la suficiencia», «la probabilidad» o la «racionalidad» de las sospechas o indicios[18].

Tanto la jurisprudencia en materia de intervención de comunicaciones como la nueva regulación legal utilizan habitualmente la expresión «suficientes indicios objetivos de la comisión del delito», pero precisar en qué consisten no resulta fácil en la práctica[19]. Con frecuencia se los ha definido como «hechos que racionalmente –mediante una valoración objetiva– son indicativos de la implicación de un sujeto en un hecho delictivo»[20].

---

[17] *Vid*. la sentencia *United States v. Hunter*, en un caso relativo al registro de ordenadores que se consideró desproporcionado *(overbreath of the search and seizure)* por no especificar la resolución judicial ni el ordenador que había de registrarse ni se refería a los indicios racionales que justificaban la medida. La sentencia es citada por RHODEN, C., «Challenging Searches and Seizures of Computers at Home or in the Office: From reasonable Expectation of Privacy to Fruit of the Poisonous Tree Doctrine», 30 *American Criminal Law Journal*, (2002-2003), pp. 107-134, p. 115.

[18] A favor de que el art. 18.3 CE incluya una referencia a los criterios que permitan diferenciar entre sospecha objetiva y conjetura subjetiva en relación con la intromisión en el derecho al secreto de las comunicaciones, se expresa ZOCO ZABALA, C., ob. cit., pp. 208 y 215. En mi opinión considero que tal definición a nivel constitucional, si bien sería positiva, tampoco serviría para delimitar los diferentes grados de sospecha, cuya calificación está estrechamente vinculada a las circunstancias de cada investigación penal.

[19] Aunque en teoría «probable comisión delictiva» implica una probabilidad más alta que la simple «sospecha razonable», y este último grado de sospecha es superior a «motivos fundados», en la práctica resulta muy difícil trazar una clara distinción entre estos diferentes grados en la probabilidad de encontrar pruebas de un delito.

[20] SSTC 171/1999, de 27 de septiembre, FJ 8; 299/2000, de 11 de diciembre, FJ 4; 14/2001, de 29 de enero, FJ 5; 138/2001, de 18 de junio, FJ 3; y 202/2001, de 15 de octubre, FJ 4, todas ellas relativas a la interceptación de comunicaciones telefónicas.

El Tribunal Supremo ha declarado en repetidas ocasiones que «la mera afirmación por parte de la policía acerca de la existencia de sospechas no es suficiente para proceder a la interceptación de las comunicaciones»[21]; y el Tribunal Constitucional, a su vez, ha indicado que «la relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan solo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido; en primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona. (...) Estas sospechas han de fundarse en datos fácticos o indicios que permitan suponer que alguien intenta cometer, está cometiendo o ha cometido una infracción grave o en buenas razones o fuertes presunciones de que las infracciones están a punto de cometerse»[22].

En definitiva, lo anterior significa que la solicitud de la medida del registro remoto de equipos informáticos debe referirse a unos hechos concretos y ha de explicar el origen de la información que sustenta las sospechas objetivas[23]. El auto judicial que autorice la medida debe valorar, sobre la base de esos hechos, si el grado de sospecha acerca de la comisión de un delito grave es suficiente para justificar la restricción de un derecho fundamental. Información anónima o que provenga de fuentes confidenciales, de ordinario, no se ha considerado suficiente para justificar dicha intromisión[24].

En alguna ocasión el Tribunal Supremo se ha enfrentado a una interesante y nada fácil cuestión: si la información obtenida a través de la cooperación internacional con unidades policiales o de inteligencia extranjeros sirve para fundamentar el suficiente grado de sospecha que justificarían la autorización de medidas investigativas restrictivas de derechos fundamentales. El caso concreto se refería a unas escuchas telefónicas, y posterior incautación de una importante cantidad de droga, sobre la base de la información transmitida a las autoridades españolas por la USA *Drugs Enforcement Agency* (DEA). En esa ocasión el abogado de la defensa adujo que la interceptación telefónica era ilícita porque las sospechas iniciales que fundaron su

---

[21] ATS de 18 de junio de 1992, que fue la primera decisión que determinaba de manera completa los requisitos para acordar una interceptación telefónica en el marco del proceso penal.

[22] STC 253/2006, de 11 de septiembre, FJ 2, citando las sentencias del TEDH *Klass and others v Germany*, de 6 de septiembre de 1978, Appl. n.º 5029/71 y *Lüdi v Switzerland* de 15 de junio de 1992, Appl. n.º 12433/86. *Vid*. también SÁNCHEZ NÚÑEZ, T., «La jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal», en *Los nuevos medios de investigación en el proceso penal. Especial referencia a la vídeovigilancia*, CGPJ, Cuadernos de Derecho Judicial, Madrid, 2007, pp. 251-299.

[23] Lo que debe reflejar el auto que autorice la medida es la fuente del conocimiento del posible delito, y a la vista de esa fuente, la fiabilidad, la concreción de los datos, etc., el juez valorará si la intromisión en la esfera de los derechos fundamentales está justificada. Así, por ejemplo, SSTC 26/2006 o 146/2006.

[24] STC 184/2003, de 23 de octubre; STC 187/2014, de 10 de marzo.

autorización no se habían obtenido a través de medios lícitos. El Tribunal Supremo sostuvo, sin embargo, que no podía presumirse que las fuentes de información policiales fueran ilícitas, y que en el presente caso no había circunstancias concretas indicativas de que la información inicial derivaba de unas escuchas ilícitas (STS 884/2012, de 8 de noviembre, RJ 2012/11360).

Las reglas y principios elaborados por nuestra jurisprudencia en materia de escuchas telefónicas son aplicables *mutatis mutandis* al registro remoto de equipos informáticos: para obtener la autorización judicial de esta medida, será preciso que previamente se lleven a cabo otras medidas de investigación *(surveillance)* con el objetivo de recabar suficientes datos que sirvan para fundar las «sospechas racionales» de la comisión de uno de los delitos para los que esta medida podría adoptarse[25]. En todo caso, siendo el registro remoto de equipos informáticos una medida nueva en nuestro proceso penal, habrá que esperar a ver cómo valoran nuestros jueces el requisito relativo a los indicios racionales de la comisión de un delito. No obstante, me aventuro a pensar que no será un criterio muy distinto del que se ha venido aplicando para las interceptaciones telefónicas.

3.2 ¿Qué equipo informático puede ser sometido a un registro remoto?

El art. 588 bis (h) LECRIM, aplicable a todas las medidas de investigación electrónicas, dispone que: «Podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.» Se trata, por tanto, de una norma de remisión a las reglas aplicables a cada una de las medidas en cuestión. Sucede, sin embargo, que, en relación con el registro remoto de ordenadores, nada se dice acerca de cuál es el ordenador que puede interceptarse a distancia, ni de los casos y condiciones en que puede someterse a registro remoto el ordenador de un tercero. Lo cual suscita dos cuestiones importantes en la práctica. Primero, si el registro remoto solo puede acordarse para acceder al ordenador del sospechoso o si puede también autorizarse para registrar el ordenador que, aun siendo de otro sujeto, posiblemente está siendo utilizado por el sospechoso para almacenar o para comunicar. Y segundo, si puede autorizarse el registro remoto del ordenador de un tercero, aunque no esté siendo utilizado por el sospechoso, pero en el cual pueden existir datos relevantes para el esclarecimiento del delito.

A este propósito, el art. 588 bis (h) LECRIM prevé la posibilidad de interceptar comunicaciones que afecten a terceras personas, en los casos y bajo las condiciones previstas para cada tipo de interceptación. En relación con la interceptación de comunicaciones telemáticas, el art. 588 ter (c) LECRIM dispone en particular:

«*Podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que:*

---

[25] En igual sentido ZOCO ZABALA, C., ob. cit., p. 212.

1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o

2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.

También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.»

¿Resulta esta norma aplicable al registro remoto de equipos informáticos? A mi juicio, la interpretación más razonable de este precepto reclama su aplicabilidad *mutatis mutandis*, en la medida en que el registro remoto de un ordenador a través de la instalación de software implica siempre una interceptación de las comunicaciones. Ello es así porque se trata de una medida que utiliza un proceso de comunicación electrónica como vía para acceder al contenido de un equipo informático. Si bien el proceso comunicativo no es el fin de esta medida –lo sería en el caso de una interceptación de las comunicaciones del ordenador en tiempo real–, sí implica una intervención en el proceso comunicativo aunque solo sea para instalar el spyware en el equipo informático objeto del registro. Podría decirse que es una medida que implica una interceptación de las comunicaciones, aunque el proceso de interceptación en sí no afecte al derecho al secreto de las comunicaciones.

En suma, si bien hay argumentos para aplicar por analogía lo dispuesto para las interceptaciones de comunicaciones, habría sido preferible que el legislador hubiera clarificado en qué condiciones puede procederse al registro remoto del ordenador de un tercero, y qué sucede si ese tercero no se encuentra en ninguna de las situaciones descritas en el art. 588 ter (c) LECRIM. A mi entender, lo importante para autorizar el registro remoto de un ordenador de un tercero es que existan motivos fundados para considerar que en dicho equipo se encuentra información relevante para la investigación, ya sea almacenada por el propio sospechoso o por un tercero, al margen de las circunstancias previstas en el art. 588 ter (c) LECRIM.

3.3 Ámbito de aplicación del registro remoto de equipos informáticos

Como ya se ha indicado, la enumeración de los delitos para los cuales puede acordarse un registro remoto de ordenadores, figura en el art. 588 septies (a) (1) LECRIM: «a) Delitos cometidos en el seno de organizaciones criminales; b) Delitos de terrorismo; c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente; d) Delitos contra la Constitución, de traición y relativos a la defensa nacional; e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.»

Este listado persigue dar cumplimento a las obligaciones asumidas por el Estado español al ratificar el Convenio del Consejo de Europa sobre la Ciberdelincuencia[26].

[26] Convenio del Consejo de Europa sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de

Conforme al art. 14 del Convenio de Budapest, los estados adoptarán las medidas legislativas «que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos» [art. 14 (1) del Convenio]. Esta obligación engloba: «a) los delitos enumerados en los arts. 2 a 11 del Convenio, y b) otros delitos cometidos por medio de un sistema informático» [art. 14 (2) (a) and (b) del Convenio]. La nueva LECRIM cumple con este compromiso y regula las medidas de investigación telemática necesarias para la persecución de delitos graves, pero también aquellos que, aún no siendo graves, se hayan cometido a través de sistemas informáticos. Algunas de esas medidas son el acceso a datos sobre el tráfico de las comunicaciones, la interceptación de las comunicaciones o el acceso a datos electrónicos almacenados en dispositivos informáticos. No obstante, el Convenio de Budapest permite a los estados formular reserva en relación con los arts. 20 y 21 del Convenio: la obtención en tiempo real de datos sobre el tráfico y sobre el contenido. Conforme al Convenio, el ámbito de aplicación de la medida relativa a la obtención en tiempo real de datos sobre el tráfico no queda limitada a un tipo de delitos, mientras que en relación con la medida del art. 21 (interceptación en tiempo real sobre los contenidos de las comunicaciones) los estados miembros solo vendrían obligados a adoptarla cuando se trate de «una serie de delitos graves que deberán definirse en su derecho interno»[27]. A pesar del sentido literal de estos dos preceptos, el Informe Explicativo del Convenio subraya que los estados deberían regular ambas medidas con el fin de luchar de manera efectiva contra los delitos informáticos y contra aquellos que implican la utilización de tecnologías informáticas. Así se lee en el para. 214 del referido Informe:

«Con todo, como la interceptación de datos relativos al contenido es un tema delicado, el Convenio deja que el ámbito de aplicación de esta medida se determine atendiendo a lo dispuesto en el derecho interno. En vista de que algunos países asimilan desde el punto de vista legal la obtención de datos relativos al tráfico con la interceptación de datos relativos al contenido, se permite la posibilidad de que puedan formular una reserva con el fin de restringir la aplicabilidad de la disposición anterior, cuya amplitud no deberá ser superior a la de la restricción impuesta por la Parte en cuanto a la interceptación en tiempo real de los datos relativos al contenido. Sin embargo, las Partes deberían considerar la aplicación de ambas medidas a los delitos establecidos por el Convenio en la Sección 1 del Capítulo II, con el fin de contar con un medio eficaz para la investigación de estos delitos informáticos y los delitos relacionados con la informática.»

En suma, el Convenio deja a los Estados miembros la libertad de definir el ámbito de aplicación de las interceptaciones en tiempo real de datos relativos al contenido, permitiendo, por tanto, que ese ámbito de aplicación se extienda solo a la investigación de delitos graves. Pero, al mismo tiempo, anima a los estados a que autoricen estas

---

2001, STE-185, conocido como el «Convenio de Budapest». España ratificó el Convenio el 3 de junio de 2010, instrumento de ratificación BOE 17 de septiembre de 2010, entrando en vigor el 1 de octubre de ese mismo año.

[27] *Vid.* también los paras. 212 y 230 del Informe Explicativo del Convenio de Budapest.

medidas en la investigación de todo delito relacionado con la informática, pues por su propia naturaleza no será posible su descubrimiento sin la interceptación del contenido de las comunicaciones en tiempo real[28].

La cuestión que se suscita en este punto, en relación con el registro remoto de ordenadores del art. 588 septies (a) LECRIM, es si esa medida permite únicamente el acceso a datos almacenados –de comunicaciones u otros contenidos– o también la interceptación en tiempo real de telecomunicaciones. El legislador español se refiere al registro remoto como la utilización de datos o códigos, o la instalación de software, que permitan «el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos». La alusión al examen del «contenido» parece implicar que no se contempla la interceptación de comunicaciones en tiempo real. Pero lo cierto es que para las comunicaciones electrónicas escritas esa distinción no tiene mucha relevancia, pues una vez enviadas –abiertas o no, leídas o no–, si no se eliminan serán almacenadas en el dispositivo y serían accesibles a través del registro remoto del mismo. En los términos del legislador español, los correos electrónicos almacenados pasan a formar parte del «contenido» del dispositivo.

Lo que intento explicar es que, como al regular el registro remoto de equipos informáticos, la ley no diferencia entre el acceso a comunicaciones y el acceso a otro tipo de datos, no resulta fácil determinar cuáles son las normas de aplicación supletoria: si las relativas a la interceptación de comunicaciones o las que regulan el registro de datos. Al permitir que el registro remoto pueda tener una duración de hasta un mes, la medida parece asemejarse más a la interceptación de comunicaciones, por lo cual parece que no sería inapropiado aplicar las normas sobre interceptación de comunicaciones. No obstante, aunque la instalación del spyware implica siempre interceptar una telecomunicación, lo cierto es que ese dataflow no es el objetivo básico o único de la medida. De ahí que el acceso remoto a un ordenador mediante la instalación de software tampoco pueda definirse como análogo a la interceptación de las comunicaciones telefónicas. Y su carácter no puede depender de lo que especifique el auto judicial autorizante, pues en muchas ocasiones el mismo no determinará qué tipo de datos son los que han de obtenerse.

Este debate no tiene un mero interés conceptual, puesto que incide directamente en el ámbito de aplicación de la medida de registro remoto, para definir en relación con qué delitos puede acordarse esta medida. La cuestión es la siguiente: la interceptación de las telecomunicaciones solo podrá adoptarse para la investigación de delitos que tengan aparejada una pena privativa de libertad de al menos tres años, además de los delitos de delincuencia organizada, terrorismo o delitos cometidos a través de sistemas informáticos. Sin embargo, el registro remoto de ordenadores solo podría autorizarse en relación con los delitos específicamente enumerados en el art. 588 septies (a)

[28] *Vid*. el Informe Explicativo paras. 211-214.

LECRIM, con independencia de la pena prevista para los mismos. Así, por ejemplo, en la instrucción de un delito cometido contra un menor, la interceptación telefónica solo podría autorizarse si el delito tuviera previsto una pena privativa de libertad de al menos tres años; mientras que el registro remoto del ordenador podría autorizarse –si se cumplen, claro está, todos los demás requisitos– aunque la pena prevista no llegara a los tres años de privación de libertad.

En mi opinión, al regular el registro remoto de equipos informáticos, la intención del legislador no ha sido cubrir también la interceptación en tiempo real de las telecomunicaciones. Por ello, aunque los correos electrónicos almacenados sean accesibles a través de esta medida, y aunque el acceso a esas comunicaciones en poco o nada se diferencia en la mayoría de los casos de su interceptación en tiempo real –y por tanto no sería irrazonable trazar una analogía entre el registro remoto de ordenadores y la interceptación de telecomunicaciones–, el ámbito de aplicación del registro remoto es el que se define en el art. 588 septies (a) LECRIM: es decir, el límite de los tres años de pena privativa de libertad no se aplica aquí.

En todo caso, en relación con los delitos cometidos a través de sistemas informáticos, la LECRIM no establece un mínimo de pena para poder autorizar la interceptación de las telecomunicaciones ni tampoco para el registro remoto de equipos informáticos. Esto, como se verá más adelante, puede plantear problemas respecto del cumplimiento del principio de proporcionalidad.

3.4 Principios de adecuación, necesidad y proporcionalidad

Como cualquier otra medida de investigación telemática que implique la restricción de un derecho fundamental, el registro remoto de equipos informáticos mediante la instalación de software ha de cumplir con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto. Estos requisitos son de sobra conocidos y existe una abundante jurisprudencia acerca de su alcance, interpretación y contenido tanto a nivel nacional, por parte de nuestro Tribunal Constitucional[29], como por parte del Tribunal Europeo de Derechos Humanos[30]. La novedad radica en que por primera vez la LECRIM no solo menciona específicamente esos requisitos, sino que además ofrece una definición de los mismos y criterios para su interpretación.

La idoneidad o adecuación se refiere a la relación entre los datos y pruebas que se pretenden obtener y las medidas acordadas para ello, esto es, si a través de la concreta medida de investigación pueden llegar a obtenerse los datos o pruebas que se persiguen y necesitan. En cuanto a la necesidad de la medida, se refiere a dos circunstancias: 1) que los datos o pruebas requeridos para el esclarecimiento del delito no sean accesibles a través de medidas menos lesivas para los derechos

[29] GONZÁLEZ BEILFUSS, M., «El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional», *Cuadernos Aranzadi del Tribunal Constitucional*, núm. 11 (2003), pp. 29 y ss.

[30] Por todos, *vid.* AA.VV., *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, J. García Roca y P. Santolaya (coords.), Madrid, 2005.

fundamentales; y 2) que sin esos datos o pruebas la investigación del delito se vería seriamente obstaculizada [art. 588 bis (a) (4) (a) y (b) LECRIM][31].

En cuanto al principio de proporcionalidad en sentido estricto –la relación entre el fin perseguido –la persecución del delito–, frente a la lesión del derecho fundamental– el legislador de 2015 indica expresamente los elementos que el juez ha de tomar en consideración a la hora de ponderar los intereses en juego, y por tanto, a la hora de decidir acerca de la proporcionalidad de una medida de investigación telemática. El art. 588 bis (a) (5) señala que las medidas de investigación telemáticas solo se reputarán proporcionadas si, después de tomar en consideración las siguientes circunstancias, el daño que sufren los derechos e intereses no es superior al beneficio para el interés público y de terceros[32]. Este criterio de ponderación es general y ya está consolidado tanto en la doctrina como en la jurisprudencia[33]. Lo novedoso, repito, es que el legislador señala expresamente cuáles son los elementos relevantes para valorar el interés público: «la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes, y la relevancia del resultado perseguido con la restricción del derecho.»

Como puede observarse, uno de esos criterios tiene significación específica en relación con las medidas de investigación telemáticas: que el delito se haya cometido en el entorno digital. ¿Qué significa esto exactamente? ¿La afectación del interés público se modula en función de si el delito se comete a través de sistemas informáticos o no? Curiosamente, el legislador indica que es un elemento para valorar el interés público, cuando lo cierto es que el hecho de que se cometa en el entorno digital en realidad no afecta al interés público sino a la mayor dificultad de esclarecer el delito en caso de que no se adopten medidas de investigación tecnológica.

El hecho de que el delito se haya cometido a través de sistemas informáticos no justifica automáticamente la adopción de una medida de investigación telemática, y tampoco la medida del registro remoto de ordenadores o dispositivos, pero sí abre la puerta a que la medida se acuerde, incluso aunque el delito no sea calificado como grave por razón de la pena. La medida podrá autorizarse si se considera necesaria

---

[31] Desde la sentencia del TEDH *Gillow v. United Kingdom*, Appl. n.º 9063/80, de 24 de noviembre de 1986, la necesidad como presupuesto para la limitación de un derecho fundamental, se interpreta como necesidad imperiosa, que tal restricción sea indispensable.

[32] Sobre los principios de suficiente previsión legal, adecuación, necesidad y proporcionalidad en relación con las escuchas telefónicas, vid., entre otras, las sentencias del TEDH *Klass and Others v. Germany*, Appl. n.º 5029/71, de 6 de septiembre de 1978; *Malone v. United Kingdom*, Appl. n.º 8691/79, de 2 de agosto de1984; *Kruslin v. France*, Appl. n.º 11801/85, de 24 de abril de 1990, y *Huvig v. France*, Appl. n.º 11105/84, de 28 de septiembre de 1995; *Kopp v. Switzerland,* Appl. n.º 13/1997/797/1000, de 25 de marzo de 1998; *Valenzuela Contreras v. Spain*, Appl. n.º 58/1997/842/1048, de 30 de julio de 1998; *Amman v. Switzerland,* Appl. n.º 27798/95, de 4 de mayo de 2000; o *Prado Bugallo v. Spain*, Appl. n.º 58496/00, de 18 de febrero de 2003.

[33] *Vid*. por todos, W. DEGENER, *Grundsatz des Verhältnismäßigkeitsprinzips und strafprozessuale Zwangsmaßnahmen,* Berlin, 1985.

porque el delito no puede esclarecerse y perseguirse a través de otros medios menos intrusivos, debido a su naturaleza «digital». Como se verá a continuación, este enfoque adoptado por el legislador de la reforma 13/2015 es acorde con los principios del Convenio de Budapest, si bien va más allá de las estrictas exigencias de ese instrumento internacional. Pero también incrementa el riesgo de un posible uso abusivo del registro remoto de ordenadores, como se hará notar más adelante.

3.5 Duración

La regla general es que toda medida restrictiva de un derecho fundamental solo podrá durar el tiempo estrictamente imprescindible para el esclarecimiento de los hechos, y así se recoge expresamente en el art. 588 bis (e) (1) LECRIM. El registro remoto de equipos informáticos solo podrá autorizarse por el plazo de un mes, prorrogable hasta un máximo de tres meses [art. 588 septies (c) LECRIM]. Conviene señalar que la duración de esta medida es mucho más limitada que la prevista para las otras medidas de investigación telemática, para las cuales de ordinario se prevé una duración de tres meses, prorrogable por iguales plazos hasta un máximo de dieciocho meses [art. 588 ter (g) LECRIM]. El legislador, además, detalla cuáles son los requisitos para solicitar y acordar la prórroga de cualquier medida restrictiva de un derecho fundamental: justificación de que la medida sigue siendo adecuada, necesaria y proporcional, sobre la base de los resultados obtenidos a medida que avanza la instrucción [art. 588 bis (f) LECRIM]. El continuo control judicial de los resultados de las medidas acordadas en los plazos establecidos por el juez [art. 588 bis (g) LECRIM] es presupuesto de la licitud de la medida. Igualmente, será ilícita cualquier prueba obtenida una vez transcurrido el plazo para el cual se autorizó la medida, incluso aunque no se advierta ni mala fe ni abuso por parte de las autoridades policiales.

El juez acordará el cese de la medida de investigación telemática una vez que desaparezcan los motivos que justificaron su adopción o que resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos. Y en todo caso, cuando haya transcurrido el plazo para el que se hubiera autorizado» [art. 588 bis (j) LECRIM]. Estas normas generales son igualmente aplicables al registro remoto de ordenadores, lo cual es plenamente positivo.

En relación con la medida de registro remoto de equipos informáticos, llama la atención que su duración se regula de manera semejante a lo previsto para las interceptaciones telefónicas, con la única diferencia de que los plazos son más reducidos: la duración ordinaria es de un mes –frente a tres– y la prórroga se limita a un máximo de tres meses, en vez de dieciocho meses. ¿Resulta razonable esta diferencia? ¿Cuáles son las razones que han llevado al legislador a establecer un plazo de un mes para llevar a cabo el registro remoto de un ordenador? Si el objetivo es permitir el acceso al contenido de un ordenador –u otro dispositivo– y obtener los datos que se almacenan en el mismo, una vez que se ha instalado el *spyware,* el registro del equipo informático y la obtención de los datos mediante clonación o *mirroring* puede realizarse en un tiempo relativamente breve. Por tanto, efectuado ese acceso y el registro con la preservación de los datos, la medida debería cesar, puesto que el objetivo para el que

se autorizó ya se ha cumplido. Lo cual debería llevar a que quienes ejecutan la medida procedieran a desinstalar o desactivar el *spyware*[34].

Sucede, sin embargo, que en ocasiones puede transcurrir cierto tiempo hasta que logra instalarse el software en el equipo que se pretende registrar, o que, una vez instalado, pasa un tiempo hasta que está operativo. Si ese tiempo se demora más de un mes no habría problemas: se solicitaría la prórroga al juez explicando los motivos por los que todavía no se ha podido acceder a los datos contenidos en el equipo que es objetivo de la medida. Pero ¿qué ocurre si transcurren más de tres meses desde que se autoriza el registro remoto y, por motivos técnicos, el software no está operativo y no se ha podido acceder a los datos? Sería el caso, por ejemplo, de que el sospechoso no hubiese abierto el ordenador en ese plazo o no hubiera activado aquellos concretos programas que permiten al spyware entrar en el sistema. ¿Debería entonces cesar la autorización o podría extenderse más allá de los tres meses máximos?

Estas cuestiones habrán de ser clarificadas en la práctica pero, de momento, ponen de manifiesto que el legislador, a mi juicio, no ha regulado de manera adecuada esta materia: por sus singulares características, la duración del registro remoto de equipos informáticos habría de establecerse tomando como punto de partida el momento en que el equipo en cuestión resulta accesible, esto es, una vez instalado y operativo el software. Si se demora la instalación, el plazo de hasta tres meses puede resultar insuficiente. Pero además, una vez instalado el software y «abierto» el ordenador al acceso remoto, puesto que los datos se «registran» por medio de clonación, la medida debería cesar una vez realizada esa clonación. En eso consiste, según lo define la propia ley, el registro remoto de un ordenador: examen sin conocimiento de su titular del contenido del mismo. Mantener el *spyware* después de haber clonado los datos especificados en la orden judicial se traduciría en una observación o interceptación del entorno digital de un sujeto por un plazo determinado. Si esto es lo que en efecto ha querido permitir el legislador, no se trataría tanto del registro de un ordenador realizado a distancia para evitar el conocimiento del titular, sino más bien de una observación de su entorno digital, a través del *hacking* de su ordenador, que podría extenderse durante un tiempo máximo.

3.6 La orden judicial

A diferencia del Reino Unido, donde el registro remoto de ordenadores puede ser autorizado por un agente de alto rango[35], en nuestro ordenamiento jurídico el registro remoto de equipos informáticos requiere autorización judicial. La competencia recae en el juez de instrucción que instruya la causa [arts. 588 bis (b) y 588 bis (c) LECRIM]. El hecho de que el mismo juez que garantiza la legalidad constitucional de las medidas

---

[34] En este sentido también BRENNER, S.W., «Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force», *Mississippi Law Journal* 81-5 (2011-2012), p. 1245.

[35] Conforme a RIPA en relación con la prevención o investigación de delitos graves (delitos sancionados con una pena privativa de libertad superior a tres años), no se requiere autorización judicial previa, vid. Abel, W., ob. cit., p. 104.

de investigación pueda acordar esas mismas medidas de oficio, no deja de ser una particularidad de nuestro sistema procesal penal, y no resulta del todo adecuado desde un punto de vista teórico: que el mismo juez que dirige la instrucción y asume la búsqueda de la verdad en el proceso penal, sea quien deba decidir que la medida que él mismo solicita cumple con todas las garantías, es cuanto menos conceptualmente cuestionable. Pese a todo, en la práctica, este sistema no suele generar problemas gracias a las garantías de independencia de los jueces en nuestro ordenamiento jurídico, junto con la continua supervisión de la fiscalía y a la existencia de un rígido sistema de exclusión de prueba ilícita *ex* art. 11.1 LOPJ[36]. El legislador de 2015 no ha alterado este esquema, en gran medida, por la falta de consenso que sigue existiendo acerca de la instauración de un nuevo modelo de instrucción penal.

En materia de registro remoto de equipos informáticos, no está claro si en casos de urgencia esta medida puede llevarse a cabo provisionalmente sin autorización judicial[37]. Desde luego la medida no puede llevarse a cabo por la policía, pero no está claro si puede ser acordada provisionalmente por el Ministro de Interior o, en su defecto, por el Secretario de Estado para la Seguridad. Al regular la interceptación de las comunicaciones, el art. 588 ter (d) LECRIM dispone:

«cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.»

---

[36] Acerca de la prueba ilícita y su exclusión, *vid*., entre otras, las SSTC 85/1994, 14 de marzo; 239/1999, 20 de diciembre; o 70/2002, 3 de abril. *Vid*. ASENCIO MELLADO, J. M., ***Prueba prohibida y prueba preconstituida,*** Madrid, 1989; del mismo autor, «La intervención de las comunicaciones y la prueba ilícita», accesible on-line en https://www.unifr.ch/ddp1/derechopenal/articulos/a_20110507_02.pdf (última entrada el 8.11.2016); GÓMEZ COLOMER, J. L., «La evolución de las teorías sobre la prueba prohibida aplicadas en el proceso penal español: del expansionismo sin límites al más puro reduccionismo. Una meditación sobre su desarrollo futuro inmediato», ***Prueba y proceso penal***, (Gómez Coloer, Ambos y Chiavario coords.), Valencia, 2008, p.116. Más reciente, recogiendo toda la jurisprudencia, PLANCHADELL GARGALLO, A., ***Prueba prohibida: evolución jurisprudencial***, Cizur Menor, 2014.

[37] En relación con el registro físico (no remoto) de un ordenador, *vid*. la controvertida STC 173/2011, en la que el TC legitima el registro por parte de la policía de un ordenador (entregado para reparar a un informático) por razones de necesidad, interpretada como urgencia. Crítica con esta sentencia se expresa RUIZ LEGAZPI, A., «Derecho a la intimidad y obtención de pruebas: el registro de ordenadores ***(Incoming de eMule)*** en la STC 173/2011», REDC núm. 100, enero-abril (2014), pp. 365-390, por considerar que no concurrían las razones de urgencia que harían imprescindible la actuación inmediata de la policía sin solicitar y esperar a la resolución judicial autorizante.

Sin embargo, esta excepción no se contempla al regular la ley los requisitos generales de la adopción de las medidas de investigación telemáticas en los arts. 588 bis (a) a 588 bis (k) LECRIM. Tampoco en el precepto específico que regula el registro remoto de ordenadores mediante la instalación de software se alude a esta excepción a la previa autorización judicial por razones de urgencia [art. 588 septies (a) LECRIM], si bien sí está previsto en relación con el registro ampliado de equipos informáticos. En virtud del art. 588 sexies (c) (3) and (4) LECRIM, «cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este», para lo cual habrán de solicitar la correspondiente autorización judicial. No obstante, en casos de urgencia «en que se aprecie un interés constitucional legítimo que haga imprescindible la medida», la policía o el fiscal podrán llevar a cabo el registro ampliado sin esperar a la autorización judicial. El juez de instrucción deberá ser informado de inmediato y como máximo en un plazo de veinticuatro horas. A la vista de la motivación, el juez confirmará o revocará la actuación del registro ampliado.

A diferencia de este precepto, el art. 588 septies (a) LECRIM no contiene una previsión similar para el registro remoto de equipos informáticos. ¿Puede entenderse entonces que estamos ante una laguna legal y que habrían de aplicarse subsidiariamente las normas sobre la interceptación de comunicaciones y el registro ampliado (que técnicamente es también un registro remoto)? ¿O, al contrario, debemos interpretar que el legislador quiso excluir expresamente la posibilidad de que los registros remotos mediante s*pyware* pudieran realizarse sin *previa* autorización judicial?

La regulación legal no es clara en este punto. Me inclino, sobre la base de la teoría constitucional de los derechos fundamentales, el principio *favor libertatis* y la efectividad de la protección de los derechos fundamentales, por una interpretación garantista, que excluya la posibilidad de instalar s*pyware* si no se ha obtenido previamente la debida autorización judicial. A pesar de que el registro remoto de equipos informáticos podría calificarse como un tipo de interceptación de comunicaciones, y por tanto no sería de suyo ilógico aplicar subsidiariamente las normas previstas para la intervención de comunicaciones telefónicas y telemáticas, creo que procede rechazar que por motivos de urgencia pueda prescindirse de la autorización judicial previa. La razón estriba en el enorme carácter invasivo del registro remoto de un equipo informático en relación con los posibles derechos afectados por esta medida: la intimidad, el secreto de las comunicaciones y la protección de datos. En casos urgentes lo apropiado sería que la policía o el ministerio fiscal cursaran una solicitud al juez de instrucción con carácter urgente. En todo caso, la orden judicial que autorice una medida de investigación telemática, siguiendo el nuevo art. 588 bis (c) LECRIM, deberá dictarse en un plazo de veinticuatro horas desde que se formuló la solicitud.

El contenido de la resolución judicial se regula de manera pormenorizada por la nueva ley en el art. 588 bis (c) (3) LECRIM[38], lo cual sin duda merece una valoración muy positiva. Esta norma ha de completarse con lo dispuesto específicamente para el registro remoto en el art. 588 sexies (c) (1) LECRIM:

«*La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.*»

4. Valoración de la necesidad, proporcionalidad y licitud de la medida

La infracción del principio de proporcionalidad, o la falta de motivación adecuada de las causas por las cuales la medida del registro remoto de un ordenador se considera proporcional, derivará en la ilicitud de la medida por infracción de los derechos fundamentales que pueden verse afectados a través de este tipo de registros: el derecho a la intimidad, el secreto de las comunicaciones, la protección de datos y, englobando a todos los anteriores, lo que se ha denominado el derecho a la *elektronische Privatsphäre*[39] o, como ha sido traducido al castellano, el derecho a la privacidad del entorno virtual o digital. Al aceptar la existencia de un derecho fundamental al entorno virtual pierden relevancia los debates dogmáticos acerca de si el registro remoto de un ordenador afecta al derecho a la intimidad (18.1 CE), al

---

[38] Art. 588 bis (c) (3) LECRIM: 3. La resolución judicial que autorice la medida concretará al menos los siguientes extremos:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

[39] En términos del Tribunal Constitucional alemán como «Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme», *Vid. Bundesverfassungsgerichtentscheidung* de 27 de febrero de 2008, accesible en www.bundesverfassungsgericht.de; Az. 1 BvR 370/07,1 BvR 595/07. Acerca del derecho al entorno virtual o digital, vid. GONZÁLEZ-CUÉLLAR, N. «Garantías constitucionales en la persecución penal del entorno digital» en Derecho y Justicia penal del siglo XXI. *Liber Amicorum en homenaje al Profesor A. González-Cuéllar García*, Madrid, 2006, pp. 1 y ss.

derecho al secreto de las comunicaciones (18.3) o a la protección de datos (18.4 CE), pues englobaría a todos ellos[40]. A su vez, el derecho al entorno virtual estaría comprendido dentro del derecho a la privacidad del art. 8 CEDH, lo cual explica que en este trabajo hayamos comenzado haciendo referencia principalmente a la privacidad. El cumplimiento del principio de proporcionalidad es uno de los requisitos esenciales para garantizar la protección de los derechos fundamentales y ha de velarse por que se observe de manera estricta en relación con las medidas de investigación telemáticas[41].

En este apartado pretendo abordar algunos de los retos a los que se enfrentan los jueces a la hora de valorar la proporcionalidad de una medida tan intrusiva como el registro remoto de un ordenador mediante *spyware*. En primer lugar analizaré la dificultad de valorar la necesidad de la medida, en particular cuando a priori la policía no sabe dónde se encuentran ubicados los datos relevantes para la investigación del delito. En segundo lugar aludiré a los problemas que se plantean en relación con la incautación de los datos electrónicos que figuran en el auto judicial que autoriza el registro. Por último mencionaré los problemas que pueden suscitarse en materia de jurisdicción en los casos en que la policía no tiene conocimiento del lugar donde se encuentran almacenados los datos que se requieren para el esclarecimiento de los hechos, los cuales podrían hallarse en el extranjero o en el ámbito de varias jurisdicciones.

4.1 Ausencia de gravedad del delito y principio de proporcionalidad de la medida de investigación

Sin duda, una de las mayores dificultades –y responsabilidades– a las que se enfrentan los jueces de instrucción a la hora de autorizar una diligencia restrictiva de

---

[40] Acerca de este derecho, *vid.* MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR, N., ob. cit., pp. 371-372, y la jurisprudencia allí citada: «la extensa y variada funcionalidad que permite cada uno de los dispositivos de almacenamiento masivo se proyecta sobre derechos de diferente significado constitucional». Vid. también Zoco Zabala, C., ob. cit., p. 47, aludiendo a que el derecho al propio entorno virtual engloba toda la información en formato electrónico.

[41] *Vid.* el Informe Explicativo del Convenio de Budapest, para. 146: «Otra salvaguardia incluida en el Convenio es que las competencias y procedimientos deberán "integrar el principio de proporcionalidad". Este principio deberá ser aplicado por cada Parte, con arreglo a los principios pertinentes de su derecho interno. Por lo que respecta a los países europeos, esto se deriva de los principios del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y las Libertades Fundamentales (1950), de su jurisprudencia aplicable y de las leyes y la jurisprudencia de cada país, que establecen que el poder o procedimiento deberá ser proporcional a la naturaleza y las circunstancias del delito. Otros Estados aplicarán los principios correspondientes contemplados en sus leyes, tales como las limitaciones respecto del alcance de las órdenes de presentación de información y de los requisitos sobre la aceptabilidad de las órdenes de registro y confiscación. Además, la limitación explícita contenida en el art. 21 que prevé que las obligaciones relativas a las medidas de interceptación relativas a una serie de delitos graves, deberán definirse en el derecho interno de cada país, constituye un ejemplo explícito de la aplicación del principio de proporcionalidad.» *Vid.* también, CANGEMI, D. «Procedural Law Provisions of the Council of Europe Convention on Cybercrime», *Inernational Review of Law, Computers and Technology,* vol.18, n.º 2, 165-171, pp. 170-171.

derechos fundamentales es la de valorar la necesidad y proporcionalidad de la misma. Ante delitos graves, una tal valoración, en principio, suele resultar más sencilla, siempre y cuando existan suficientes sospechas objetivas de la comisión de ese delito grave. En general, cuando se trate de delitos de criminalidad organizada transnacional y terrorismo, o delitos cometidos contra menores y personas incapaces, la restricción del derecho a la privacidad estará legitimada, incluso a través del registro remoto de equipos informáticos. Ahora bien, cuando estamos ante delitos cometidos a través de sistemas informáticos la aplicación del principio de proporcionalidad ya no resulta tan fácil, sobre todo porque el perjuicio que esos delitos causan a la sociedad no siempre resulta tan evidente. En esos casos, en los que la pena prevista para el delito no es elevada, la gravedad del delito no justifica *per se* el sacrificio de los derechos fundamentales de los individuos. Entonces, ¿cuál es el motivo que ha inducido al legislador a autorizar una medida tan invasiva como es el *hacking* de un ordenador y el registro de su contenido para delitos que no se consideran graves?

En este punto parece producirse una desvinculación entre los conceptos de interés público y gravedad del delito: el legislador entiende que puede haber un interés público que justifique la injerencia en derechos fundamentales incluso para perseguir un delito que el propio legislador no considera grave.

La respuesta, como adelantábamos más arriba, y como se explicita en el Convenio de Budapest, se encuentra en la valoración de la necesidad de la medida: por sus peculiares características, la inmensa mayoría de los delitos informáticos no podrán descubrirse –y por tanto quedarán impunes– a menos que se autoricen medidas de investigación telemática. El interés público deriva precisamente del fin legítimo que es evitar una tal impunidad generalizada, que en última instancia llevaría a que internet se convirtiera en un territorio al margen de la ley. No es irrazonable tolerar la posibilidad de restringir derechos fundamentales de tanta importancia para la persona a pesar de que el delito cometido no pueda definirse como grave por razón de la pena que el código penal le atribuye[42]. Los peligros a los que se enfrenta el «ciudadano global» justificarían ese planteamiento, que de suyo no me parece objetable. No obstante, se trata de una perspectiva no exenta de controversia, y prueba de ello es, por ejemplo, la cuestión prejudicial formulada por la Audiencia Provincial de Tarragona ante el Tribunal de Justicia de la Unión Europea, en relación con la interpretación del principio de proporcionalidad en esta clase de situaciones[43].

---

[42] En relación con intervenciones telefónicas el Tribunal Constitucional ya ha determinado que el requisito de la proporcionalidad no exige necesariamente que el delito investigado sea grave por razón de la pena, puesto que la gravedad del mismo puede derivar de otros elementos, al margen de la pena atribuida. En este sentido, *vid.,* por ejemplo, las SSTC 299/2000, de 11 de diciembre de 2000, y la STC 82/2002, de 22 de abril de 2002.

[43] Aunque esta cuestión prejudicial se formula en relación con el registro de un teléfono móvil y los hechos tuvieron lugar antes de la entrada en vigor de la Ley Orgánica 13/2015, de 5 de octubre, esta cuestión muestra la preocupación de los jueces a la hora de valorar la proporcionalidad de las medidas de investigación tecnológicas. *Vid.* http://www.iustel.com/diario_del_derecho/, of 8 abril 2016.

Lo anterior no significa que el juez deba necesariamente acordar un registro remoto de ordenadores a través de *spyware* en los casos en que la ley lo autoriza por haberse cometido el delito a través de sistemas informáticos y existan sospechas fundadas acerca de la comisión del mismo. Antes de autorizarlo, el juez de instrucción habrá de ponderar todos los elementos para apreciar si la medida, en el caso concreto, cumple con el principio de proporcionalidad. En primer lugar, habrá de sopesar la gravedad del hecho delictivo, tomando en consideración no solo la pena prevista, sino también la actuación del principio de prevención general y especial, además del daño que esas conductas están causando a la sociedad y a un sujeto en particular.

4.2 El registro remoto de equipos informáticos como medida excepcional

En segundo lugar, el juez habrá de comprobar si las pruebas que se prevé obtener a través de la medida de investigación son realmente relevantes para el esclarecimiento del hecho, porque no existen otras pruebas. Y, finalmente, debe confirmar que las pruebas o datos requeridos no pueden conseguirse con medidas menos lesivas de los derechos fundamentales. Estos elementos de la ponderación en materia de restricción de derechos fundamentales en el marco de un proceso penal son bien conocidos, y por ello no me extiendo aquí en su desarrollo.

Lo que sí me interesa destacar aquí es cómo inciden esos elementos en la apreciación de la proporcionalidad de la medida del registro remoto de equipos informáticos: en concreto, cuándo puede reputarse esta medida efectivamente necesaria para la obtención de unos datos electrónicos. La cuestión es importante, porque el *hacking* de un ordenador solo podrá considerarse proporcionado si es estrictamente necesario, como consecuencia de que los datos que se buscan no son accesibles por medios menos lesivos de los derechos fundamentales. Compete al juez de instrucción pronunciarse sobre la necesidad de la medida: en ocasiones podrá exigir que, antes de autorizar un registro remoto de equipos informáticos, se intente obtener los mismos datos por otras vías; mientras que otras veces podrá descartar directamente la posibilidad de emplear medios menos lesivos. Al respecto carecemos en España de suficientes estudios empíricos y las resoluciones judiciales –sobre todo en materia de interceptaciones telefónicas– no siempre aluden a la ausencia de otras medidas de investigación que llevarían a resultados análogos o equivalentes. A pesar de ello, ha de insistirse en que tanto la jurisprudencia constitucional española como la del TEDH exigen que se cumplan esos principios de necesidad y proporcionalidad, y que tal cumplimiento quede reflejado adecuadamente y de manera suficientemente concreta en la resolución judicial. Deben evitarse fórmulas genéricas del tipo «considerando que los datos son necesarios para la investigación de los hechos y que no puede accederse razonablemente a los mismos a través de medios menos invasivos, etc.» Tales fórmulas terminan por vaciar la verdadera garantía de la excepcionalidad de estas medidas.

Aplicando lo anterior a la cuestión que aquí nos ocupa, parece que el acceso remoto a los datos del ordenador solo debería autorizarse si la policía no logra determinar la localización física de esos datos, pues solo entonces devendría necesario el acceso

por vía remota. Si se sabe dónde se encuentran los datos y se puede acceder a ellos directamente mediante el registro del dispositivo de almacenamiento, la medida de entrada y registro, complementada con la autorización para registrar el ordenador, haría innecesario recurrir al acceso remoto del ordenador mediante *spyware*. En este punto creo importante subrayar que el acceso remoto de un ordenador mediante la instalación de software es una medida sin duda más invasiva la esfera de privacidad que el registro directo de ese ordenador, aunque para este último sea preciso solicitar también la entrada y registro en un lugar cerrado, por practicarse sin conocimiento del afectado.

En consecuencia, si el ordenador es accesible para ser registrado «físicamente», en principio, si se admite la premisa anterior –mayor lesividad del registro remoto por ser una medida clandestina– no debería autorizarse su acceso remoto a través de la instalación de software. Clarificado este extremo, queda todavía la cuestión relativa a si el juez de instrucción, antes de autorizar el registro remoto, debe confirmar que la localización física del ordenador no es posible; o si, aun pudiendo acceder al equipo informático directamente, las circunstancias de la investigación requieren que el sospechoso no tenga conocimiento de tal registro. Parece que tal justificación de la necesidad de la medida sería posible; pero, de nuevo, sería una circunstancia que, por ser excepcional, debe ser cuidadosamente motivada en el auto judicial.

4.3 Alcance extraterritorial del registro remoto de equipos informáticos

Aún es preciso dilucidar una última cuestión a la que habrán de enfrentarse los jueces a la hora de acordar el registro remoto de equipos informáticos, y que se refiere a la localización de los datos electrónicos. Cuando los datos no sean accesibles a través del registro directo del ordenador por encontrarse archivados en un equipo informático ubicado en el extranjero, o en la nube, o en servidores situados fuera de las fronteras nacionales (en uno o más servidores), ¿cómo debería proceder el juez de instrucción? ¿Podría autorizar el registro remoto extra-territorial, sobre la base de que la legislación española no lo prohíbe expresamente? ¿O debería denegar tal medida, siguiendo los principios establecidos en el Convenio de Budapest, cuya normativa se refiere solo a la obligación de los estados de facilitar el acceso a los datos almacenados «en su territorio»?[44]

El acceso a ordenadores o a datos almacenados en otro estado es una medida que como regla se ha entendido que afecta a principios de soberanía y a las reglas que rigen las relaciones internacionales, en concreto la *international comity*. No es, por ello, un tema que pueda tomarse a la ligera[45]. El hecho de que la tecnología permita

---

[44] *Vid*. los arts. 19, 20 y 21 del Convenio de Budapest en los que se alude siempre al propio territorio del estado parte. Conforme al Convenio, el acceso transfronterizo de datos electrónicos a través de registros remotos, solo se contempla: 1) previo consentimiento de la persona titular de esos datos; o 2) se pueden acceder sin consentimiento aquellos datos de acceso abierto o público *(open source or publicly available data)* con independencia de dónde se encuentren geográficamente almacenados (art. 32 del Convenio de Budapest).

[45] *Vid*. GOLDSMITH, J. L., «The internet and the legitimacy of the remote cross-border searches», *University Chicago Law Review* (2001), pp. 103-118.

acceder a datos electrónicos más allá y con independencia de las fronteras territoriales no significa automáticamente que tal acceso deba autorizarse, aunque para algunos autores la propia transnacionalidad de los datos electrónicos no debería verse afectada por las barreras nacionales, esto es, en función del lugar donde se localicen geográficamente los datos o el servidor que aloja esos datos[46].

En este sentido, una vez más, la regulación de la LECRIM en materia de registro remoto de ordenadores mediante *spyware*, resulta excesivamente parca y ambigua. Quizás esta falta de claridad haya sido deliberada, a la espera de lo que puedan disponer futuros convenios internacionales o lo que se establezca en materia de procesos penales transnacionales en la Unión Europea, como la Directiva sobre la Orden Europea de Investigación[47].

En los Estados Unidos de América, el art. 41 (b) de las *Federal Rules of Criminal Procedure* contiene una clara limitación territorial: mediante el registro remoto de ordenadores solo se podrá acceder a equipos que se hallen en el distrito judicial en el que se ha emitido la orden judicial. Esta limitación territorial genera numerosos problemas en la práctica, debido fundamentalmente a que la policía al solicitar al juez la medida en la mayoría de las ocasiones no puede determinar dónde se ubican los datos que han de obtenerse. Esa es la causa de que se haya solicitado la reforma de este precepto. En el momento de escribir este trabajo, se está debatiendo la correspondiente reforma legislativa que permitiría la autorización de registros remotos más allá del distrito judicial en el que se ha emitido la orden[48].

Por otro lado, si la ley del estado en el cual se encuentran ubicados los datos no contempla la posibilidad de que autoridades extranjeras lleven a cabo registros

---

[46] Así, VELASCO NÚÑEZ, E., «Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica», ***Diario La Ley***, n.º 8183, 4 de noviembre de 2013, pp. 1-24, pp. 12-13: «La deslocalización –la energía y los paquetes de datos informáticos y telecomunicativos (ceros y unos) se producen en un punto geográfico que deja de estar geolocalizado de inmediato aunque lo gestione una operadora que sí lo esté– y la transnacionalidad –circulación a través del espacio de más de un Estado soberano–, no son variables que afecten a los derechos fundamentales, y por lo tanto a la licitud de la prueba a que se refiere el art. 11.1 LOPJ. La tutela de los derechos fundamentales no puede quedar a la decisión del gestor de un servicio informático (ejemplo de Google) sobre el lugar que elija para ubicar los medios técnicos desde los que lo presta, máxime cuando opera –y la infracción penal produce efectos dañinos– en el país que trata de perseguir el delito, cuando los dispositivos/terminales se hayan ocupado y el delito haya producido efectos, por ejemplo, en España.» A favor de un replanteamiento de la actual concepción de territorialidad y de la jurisdicción al referirnos al ciberespacio, se expresa también, Ortiz Pradillo, J. C., ob. cit., p. 278.

[47] *Vid*. art. 31 de la Directiva 2014/41/UE, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, DO1.5.2014, L 130/1.

[48] *Vid*. por ejemplo, BENEMANN, D. R. y Elm, D. L., «Extraterritorial Search Warrants. Rule Change», *Criminal Justice* 29 (2014-2015), p. 10. Sobre la problemática de la aplicación de los registros remotos de equipos informáticos en los diferentes Estados de los EE.UU., debido al diverso alcance que tiene la Cuarta Enmienda en cada uno de ellos, vid. BRENNER, S.W., «Law, Dissonance, and Remote Computer Searches», *North Carolina Journal of Law & Technology*, vol. 14-1 (2012-2013), pp. 60 ss.

remotos en su territorio, tal medida no cumpliría con la *lex loci.* Esto significa que, siendo esa medida ilícita en el estado de ejecución, la admisibilidad de la misma en el estado del fuero podría cuestionarse. La admisibilidad de la prueba transnacional es un tema discutido ampliamente, sobre todo en el ámbito de la Unión Europea, pero no es este el lugar de abordarlo. Baste subrayar aquí que, debido a que el registro remoto es una medida que fácilmente puede ejecutarse extraterritorialmente –y que de ordinario no requiere la cooperación de las autoridades del estado de ejecución–, es donde con más cuidado han de revisarse los principios y normas que deben aplicarse a la admisibilidad de la prueba transnacional.

La Ley 13/2015 no regula estas cuestiones, lo cual obligará a los jueces a realizar una interpretación integradora del art. 588 septies LECRIM, para la cual no hay pautas preestablecidas, puesto que el registro remoto de equipos informáticos es una medida nueva y no hay precedentes jurisprudenciales acerca de la extensión extraterritorial de una medida de investigación acordada por un juez español. Por ello, ya he insistido en la necesidad de abordar la regulación del proceso transnacional, especialmente en lo que respecta a las normas relativas a la prueba transnacional, con el fin de garantizar el respeto de las garantías fundamentales del proceso penal.

Las implicaciones extraterritoriales obligan a insistir nuevamente en que, al ser el registro remoto de ordenadores una medida tan intrusiva, solo debería autorizarse con carácter excepcional, y, en principio, solo cuando la incautación directa de los datos no sea posible. Hubiera sido deseable que así se hubiera señalado en la propia ley, con el fin de evitar el riesgo de un uso abusivo de esta medida simplemente porque resulte más rápido o económico que localizar el ordenador y proceder a su registro físico.

4.4 Registro e incautación de los datos electrónicos y el principio de proporcionalidad

Tanto si se realiza directamente como mediante la instalación de software, el registro de un equipo informático plantea la cuestión –compleja– de cuáles son los datos que han de ser incautados al efectuar el registro. A estos efectos, como regla, no hay diferencias notables entre un registro directo y el que se hace on-line, salvo el tiempo que se puede emplear en copiar y seleccionar los datos. El art. 588 septies (a) (2) (b) LECRIM señala que la resolución judicial autorizando el registro remoto especificará, entre otros:

«*El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.*»

Y en el apartado (d) de este mismo precepto:

«*La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.*»

La intención del legislador es loable, pues confiere al juez de instrucción el control no solo de la procedencia de la medida, por su necesidad y proporcionalidad, sino también

el modo en que se ejecutará la misma, indicando la duración y los plazos para someter los resultados a su control, así como el tipo de software que se instalará en el terminal a registrar, el modo en que serán aprehendidos los datos y también si los agentes pueden realizar copias de esos datos y, en tal caso, cómo habrán de conservarse para garantizar su autenticidad e integridad. Ahora bien, aunque esta regulación legal no merece objeción alguna, lo cierto es que en la práctica, y salvo excepciones, los jueces de instrucción no tienen conocimientos de informática suficientes para decidir cuál es el software que debe utilizarse para el registro remoto o cómo debe realizarse la copia y conservación de los datos que se aprehendan. Al respecto, y en tanto los jueces de instrucción no reciban formación especializada en estas materias y se elabore un protocolo de ejecución de estas medidas, habrán de confiar en las indicaciones que reciban de los propios agentes especializados en delitos telemáticos o en peritos informáticos.

Al margen de esta cuestión meramente práctica, hay otro aspecto de la ejecución de tal medida que suscita dudas en cuanto a la proporcionalidad, y es la referida a los datos a incautar. En los registros físicos de domicilios y otros espacios cerrados, solo los elementos que estén relacionados con el hecho delictivo investigado podrán ser objeto de aprehensión. Pero el registro de un ordenador presenta características propias: los «objetos» relacionados o relevantes para la investigación no son directamente visibles, y el modo en que se almacenan los datos no siempre permite identificar cuáles son relevantes: datos que resultan absolutamente irrelevantes para la investigación pueden estar archivados en las mismas carpetas o archivos que aquellos que constituyen pruebas decisivas.

Con frecuencia, en el registro de un equipo informático será preciso utilizar programas específicos de búsqueda para identificar cuáles son los archivos que interesan para la investigación porque contienen datos relevantes. Como la cantidad de datos puede ser ingente, sin esas herramientas de búsqueda no sería posible aislar los datos que se requieren. Y para ello, en muchas ocasiones no habrá más remedio que registrar todos los datos, aunque en el auto judicial solo se autorice la incautación de unos concretos datos. Debido a que los datos electrónicos son volátiles, para llevar a cabo ese filtrado y seleccionar los datos relevantes, en la práctica con frecuencia lo que se realiza es una clonación de todo el contenido del ordenador. Una vez clonados los datos, se procede a realizar el filtrado. En particular, en el registro remoto de equipos informáticos la clonación se realiza cuando se ha accedido mediante el *spyware* al ordenador, y el filtrado de los datos se lleva a cabo después de que se hayan transferido a los equipos de la policía[49]. Como puede observarse, resulta imposible aquí una analogía con el registro domiciliario: equivaldría a llevarse todos los objetos, papeles o enseres y después seleccionar los relevantes, lo cual sería claramente desproporcionado. Pero tampoco resulta posible una analogía con el clonado de datos desde un ordenador al

[49] No obstante, también es posible que en el proceso de clonación se utilice ya software específico para que solo se incauten determinado tipo de archivos, esto es, el filtrado se realice ya on-line.

cual se ha accedido físicamente, pues ese clonado se realiza en presencia del secretario judicial y el encausado puede también estar presente[50].

Si el registro de los datos electrónicos de un equipo informático suele efectuarse una vez que se ha clonado el contenido del mismo, el siguiente paso es determinar cómo debe procederse al filtrado de esos datos. ¿Cómo se separan los archivos o datos relevantes de aquellos otros que no tienen relación alguna con el delito investigado? ¿Quién y en función de qué criterios realiza la selección de los datos? ¿Deben revisarse todos los datos contenidos en el ordenador, para asegurarse de que la búsqueda es exhaustiva y no se quedan datos o información relevante sin identificar? ¿Qué software ha de utilizarse para la búsqueda de datos? ¿Deben utilizarse estas herramientas de búsqueda con una definición limitada de los datos a obtener?

En términos abstractos, la respuesta a todas estas cuestiones es muy sencilla: todos estos extremos deberá especificarlos el juez en el auto autorizando la medida. Pero, esto nos lleva a la cuestión de cómo precisar el contenido de ese auto. Comenzando por la última cuestión, ha de reconocerse que delimitar la búsqueda mediante el empleo de determinadas palabras clave, o dirigiendo la búsqueda a determinado tipo de archivo, puede ser útil para encontrar los datos que interesan. No obstante, este método de búsqueda también puede tener como consecuencia que ciertos datos que son importantes para la investigación criminal, no sean detectados. Limitar el acceso a los datos a través de *searching tools* no parece adecuado en todos los casos, pues puede impedir que datos relevantes sean efectivamente aprehendidos.

Si se descarta el filtrado a través de software o palabras clave, habrá de establecerse alguna otra forma que permita preservar la privacidad de todos aquellos datos electrónicos que han sido aprehendidos y que no están relacionados con la investigación. La dificultad estriba, nuevamente, en separar unos de otros y en determinar quién debe llevar a cabo la identificación de los datos que, por ser relevantes, encuentran cobertura en la autorización judicial.

El modo de llevar a cabo la selección de los datos es de suma importancia para que el registro de un equipo informático no infrinja el principio de proporcionalidad. Ha de tenerse en cuenta que este tipo de registros no solo afecta a la privacidad del denominado entorno electrónico de un individuo –intimidad, secreto de las comunicaciones y protección de datos– sino también al derecho a la privacidad de otras muchas personas no relacionadas con el delito y que simplemente se han comunicado con el sujeto investigado, figuran en su facebook, o están conectadas en algún chat.

La Ley 13/2015 subraya que toda medida de investigación telemática ha de respetar los principios de especialidad y de proporcionalidad, pero no ofrece pautas para dar cumplimiento a esos principios al ejecutar una medida de registro remoto. Es cierto que el legislador expresamente establece que la resolución señalará si los agentes pueden realizar copias y conservarlas, además de especificar las medidas a tomar

---

[50] *Vid.* VELASCO NUÑEZ, E., ob.cit, p. 14; MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR, N., ob. cit., p. 375.

para preservar la autenticidad e integridad de los datos. Pero a esta previsión legal ha de dársele contenido: son reglas generales que necesitan ser concretadas a la hora de llevar a cabo el registro de un ordenador.

El principio de proporcionalidad puede verse infringido tanto en el momento de proceder a la autorización de la medida como en la fase de ejecutarla, y respecto de esta última poco o nada se especifica en la ley; todo ello ha de ser definido y delimitado en la resolución judicial *ad hoc*, pero no se ofrece a los jueces de instrucción pautas que les indiquen cómo delimitar esa ejecución para que sea respetuosa con el principio de proporcionalidad[51]. Al mismo tiempo, es importante recordar la volatilidad de los datos electrónicos, lo cual obliga a adoptar rápidamente medidas de conservación de los datos para evitar su destrucción. Como consecuencia, ha de descartarse la posibilidad de que los agentes al cargo del registro remoto realicen un filtrado minucioso de los datos relevantes antes de proceder a copiar los archivos.

El proceso de ordinario tendrá lugar a la inversa: primero se procederá a clonar el contenido y después se seleccionarán los datos relevantes para la investigación, sin que previamente queden eliminados de esa aprehensión datos que afecten al núcleo de la intimidad del individuo[52]. Esto es lo que parece razonable, desde el punto de vista práctico, si las capacidades tecnológicas lo permiten, claro está.

Pero ¿resulta este modo de proceder compatible con la jurisprudencia del TEDH en materia de proporcionalidad de los registros domiciliarios? Si trazamos una analogía con los documentos que pueden incautarse durante un registro domiciliario, la clonación del ordenador equivaldría a incautar todos los documentos. La sentencia del TEDH en el caso *Niemietz v Germany* es particularmente ilustrativa en este sentido[53]: se estimó que el registro del despacho profesional de un abogado, vinculado al delito investigado, había vulnerado el art. 8 del CEDH, precisamente por haberse aprehendido un número elevado de carpetas no relacionadas con el delito ni relevantes para la investigación. El Tribunal Europeo de Derechos Humanos declaró en esa sentencia que el principio de proporcionalidad se había visto conculcado y la medida se había ejecutado en infracción del art. 8 CEDH. La cuestión es si esta jurisprudencia es aplicable también a los registros remotos –y los no remotos– de ordenadores. Si respondemos afirmativamente, la consecuencia sería que no es legítimo clonar el contenido del ordenador y habría que seleccionar previamente los datos relevantes

---

[51] En la jurisprudencia de los Estados Unidos, para valorar la proporcionalidad de la medida del registro del contenido un ordenador al cual se ha accedido físicamente, se toman en cuenta fundamentalmente tres elementos: «(1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers could differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the ítems more particularly in light of the information available to it at the time the warrant was issued, sentencia ***United States v. Lacy***, 119 F.3d 742, 746 n.7 (9th Cir. 1997), ***cert. denied***, 523 U.S. 1101 (1998). Sentencia citada por RHODEN, C., ob. cit., p. 115.

[52] W. ABEL, ob. cit., p. 103.

[53] STEDH *Niemietz v Germany*, de 16 de diciembre de 1992, Appl. N.º 13710/88.

para la investigación; de manera que todos los registros en los que se clonaran los datos estarían vulnerando el principio de proporcionalidad. Lo anterior me lleva a concluir que, para valorar la proporcionalidad del registro remoto de un ordenador y la aprehensión de los datos electrónicos, no pueden aplicarse los mismos parámetros que se utilizan en relación con los registros domiciliarios y la incautación de documentos.

Dicho lo anterior, todavía ha de resolverse la cuestión que antes planteaba: cómo separar los datos relevantes para la investigación penal de aquellos que no lo son. ¿Cómo preservar el derecho a la intimidad de ciertos datos que no están relacionados con el delito? La respuesta no se encuentra en la Ley 13/2015. En relación con la interceptación de las comunicaciones, nuestros tribunales han sido muy estrictos a la hora de exigir que, para el cumplimiento del control judicial de esta medida, todo el material interceptado debe ser entregado al juez de instrucción, sin que la policía pueda proceder a la selección de las conversaciones relevantes, y todo ese material debe ponerse a disposición de la defensa (salvo aquellas conversaciones que afecten al núcleo del derecho a la intimidad)[54].

Si trasladamos esos criterios al registro de un equipo informático, la consecuencia sería que todos los datos electrónicos aprehendidos deberían transmitirse al juez de instrucción. Esto conllevaría ciertos problemas prácticos. En primer lugar, la enorme cantidad de datos que recibiría el juez hace imposible en la práctica que éste pudiera controlar el modo en que se ha efectuado la selección de los datos. Y en segundo lugar, si tuviera que revisar esos datos, el juez necesitaría formación específica o bien la asistencia de un perito informático.

Con frecuencia se ha querido trazar una analogía entre el registro de objetos físicos en un espacio cerrado y el registro de datos electrónicos contenidos en un ordenador. Y si bien, a la postre, la diferencia entre un documento en papel y en formato digital se encuentra básicamente en el tipo de soporte, lo cierto es que la comparación no es válida. Y ello, no tanto por una cuestión cualitativa –que también tiene su importancia– sino sobre todo por la dimensión cuantitativa: un equipo informático almacena ingentes cantidades de datos sobre la vida de su usuario, de tal forma que aprehender y conservar todos los datos almacenados en ese equipo mediante el clonado del mismo claramente superaría los límites de la investigación de un concreto delito. En teoría, de acceder a esa enorme cantidad de información se abriría la posibilidad de llevar a cabo a una especie de *inquisito generalis* sobre la persona investigada, pues podría reconstruirse prácticamente la mayor parte de su vida privada, al menos en las sociedades occidentales.

Precisamente, las normas del proceso penal, tanto las relativas a la incoación de la instrucción como las relativas a la prueba, persiguen minimizar el riesgo de conferir al

[54] Art. 588 ter (i) LECRIM. Los tribunales alemanes también han declarado que la selección de los datos relevantes para el proceso debe realizarse por la autoridad judicial, incluyendo este concepto también al ministerio fiscal y al letrado judicial, pero no a la policía.

estado unos poderes tales que pueda ejercer un absoluto control sobre la vida de los ciudadanos. Todo sistema democrático debe evitar ese exceso de poder del estado, pero, en el caso que nos ocupa, ¿cómo articular el registro remoto para que no se convierta en una medida que permita investigar la vida completa de una persona?

Sin ánimo de proponer una solución definitiva, hay dos medios que pueden resultar de utilidad, cuando el filtrado inicial de datos no pueda realizarse mediante software específico, sino que no quede otra alternativa que clonar el contenido del ordenador. El primero consistiría en designar una autoridad independiente para que realizara el filtrado de los datos aprehendidos y excluyera de los autos aquellos que no estuvieran cubiertos por la autorización judicial por no tener vinculación con el hecho delictivo investigado. La otra posibilidad consistiría en impedir que los datos no relacionados con los hechos investigados pudieran ser empleados como prueba en relación con otros delitos; en otras palabras, restringir la posibilidad de utilizar los descubrimientos casuales como prueba de otros delitos. De momento, ninguna de estas opciones ha sido acogida por la Ley 13/2015.

En materia de hallazgos casuales –datos relativos a la comisión de un delito descubiertos casualmente durante la ejecución de una medida acordada para la investigación de otro delito– ha de recordarse que, hasta la reforma operada por la Ley 13/2015, la LECRIM no contenía regulación alguna. En sede de medidas de investigación telemática, el nuevo art. 588 bis (i) LECRIM se limita a realizar una remisión a lo dispuesto en el art. 579 bis LECRIM (descubrimientos casuales en relación con la apertura de correspondencia). En este precepto solo se indica que los descubrimientos casuales podrán ser utilizados como medio de investigación o prueba en otro proceso penal previa autorización judicial, que habrá de comprobar las circunstancias en que se obtuvo esa prueba y su legalidad. Pero el legislador no aporta ulteriores detalles acerca de cuál sería su eficacia y valor probatorio.

En suma, el legislador ha obviado los problemas que la adopción de un registro remoto de equipos informáticos –y también el no remoto– plantea desde la perspectiva del principio de proporcionalidad. De manera que serán los tribunales los que habrán de poner especial cuidado para que en la ejecución de esta medida de investigación no se vulneren las garantías constitucionales. Es de desear que no se siga la práctica extendida en materia de escuchas telefónicas, donde se acepta que la motivación del auto judicial consista en una remisión a los datos que constan en el informe policial o del ministerio fiscal[55]. No solo la autorización del registro remoto de un ordenador a través de s*pyware* debe cumplir escrupulosamente con el principio de proporcionalidad, y expresarse así en el auto correspondiente, sino que debe evitarse que la ejecución de esta medida sirva como vía de entrada para investigar la vida entera de una persona.

[55] Por ejemplo, STC 25372006 o STS 248/2012, de 2 de abril.

5. A modo de conclusión

La injerencia por parte del Estado en el derecho a la privacidad de las personas a través del registro de un equipo informático requiere que ese registro esté sujeto a límites claros y controles efectivos, que deben ser aún más estrictos cuando el acceso se produce de manera clandestina mediante la instalación de *spyware* que permite acceder y copiar el contenido de un ordenador sin conocimiento de su titular. Si bien esta medida es necesaria para la investigación de determinados delitos, y el legislador ha delimitado para qué tipos de delitos puede acordarse, es preciso insistir en su carácter excepcional: solo es legítima cuando es estrictamente necesaria porque medidas menos invasivas no permitirían obtener los datos requeridos para el esclarecimiento del hecho delictivo.

La reforma introducida por la Ley 13/2015 regulando las medidas de investigación telemática debe sin duda ser bienvenida, al promover no solo una mayor seguridad jurídica, sino también una más eficaz lucha contra la delincuencia.

En relación con el registro remoto de equipos informáticos mediante la instalación de *spyware*, el legislador se ha mostrado valiente al dar un paso significativo en materia de investigación telemática. La reforma de la LECRIM apuesta así por la modernización de la instrucción penal en España, adaptándose no solo a las legislaciones más avanzadas de nuestro entorno, sino dando también cumplimiento a las recomendaciones del Consejo de Europa [Rec CM(95)13] y a las obligaciones internacionales asumidas. La reforma merece ser elogiada también por el alto grado de calidad legislativa y por el esmero que ha puesto el legislador en detallar todos los requisitos que han de cumplirse para garantizar los derechos fundamentales.

Ahora bien, al introducir una medida nueva y tan intrusiva como el acceso y registro remoto de equipos informáticos, deberían extremarse las cautelas para que ese difícil equilibrio entre el interés público en la persecución eficaz del delito y el respeto de los derechos fundamentales de los individuos no se rompa en perjuicio de estos últimos. En este contexto, se echa en falta un protocolo para garantizar el cumplimiento del principio de proporcionalidad en la ejecución de esta medida. Aunque la ley expresa cuáles son los criterios para valorar la proporcionalidad de todas las medidas de investigación telemáticas, se trata de criterios que, al ser generales, dejan muchas preguntas sin responder.

Por ello, ahora más que nunca es vital que los jueces extremen el rigor en la motivación de los autos que autoricen una medida de registro remoto de un equipo informático, con una escrupulosa descripción de la necesidad de la medida y su proporcionalidad. Esa motivación es la que permitirá a su vez controlar el precio que los ciudadanos pagaremos en concepto de privacidad a cambio de combatir la ciberdelincuencia y otras formas de delitos graves.

Que los troyanos se conviertan en los nuevos agentes que investigan el delito puede admitirse excepcionalmente, pero en ningún caso es aceptable que se conviertan en una vía subrepticia para que el Estado acceda a los datos de la entera vida de un

ciudadano sometido a la investigación de un delito (que ni siquiera tiene, además, que ser un delito grave). Permitir el acceso a todos los datos que contiene un ordenador podría abrir la puerta a investigaciones prospectivas, a que el Estado caiga en la peligrosa tentación de escrutar toda la vida de una persona. Con ello no solo correría peligro nuestra privacidad, sino el propio estado de derecho.

BIBLIOGRAFÍA

AA.VV., *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos,* J. García Roca y P. Santolaya, (coords.), Madrid, 2005.

ABEL, W., «Agents, trojans and tags: The next generation of investigators», 23 *International Rev. of Law Compu*ters *& Technology*, vol. 23 (March) 2009, pp. 99-108, p. 103.

AGUILERA MORALES, M., *Proceso penal y causa general*, Madrid 2008.

BRAUN, F., «Ozapftis–(Un)Zulässigkeit von Staatstrojanern», *Kommunikation und Recht,* 11/2011, pp. 681-686.

BENEMANN, D.R., y ELM, D.L., «Extraterritorial Search Warrants. Rule Change», *Criminal Justice* 29 (2014-2015), p. 10.

BÖCKENFÖRDE, T. «Auf dem Weg zur elektronischen Privatsphäre», *Juristenzeitung,* 19/2008, pp. 925-939.

BUENO DE MATA, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», *La Ley*, n.º 8627, 19 octubre 2015.

BRENNER, S.W., «Law, Dissonance, and Remote Computer Searches», *North Carolina Journal of Law & Technology,* vol. 14-1 (2012-2013), pp. 60 y ss.

BRENNER, S.W., «Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force», *Mississippi Law Journal*, 81-5 (2011-2012), pp. 1229-1261.

CANGEMI, D. «Procedural Law Provisions of the Council of Europe Convention on Cybercrime», *Inernational Review of Law, Computers and Technology*, vol. 18, n.º 2, 165-171.

DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», *La Ley,* n.º 8693, 2 febrero 2016, pp. 1-14.

GARCÍA SAN MARTÍN, J., «Consideraciones en torno al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», *La Ley,* n.º 8468, 28 enero 2015.

GOLDSMITH, J.L., «The internet and the legitimacy of the remote cross-border searches», *University Chicago Law Review* (2001), pp. 103-118.

GONZÁLEZ BEILFUSS, M., «El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional», *Cuadernos Aranzadi del Tribunal Constitucional*, núm. 11 (2003), pp. 29 y ss.

GONZÁLEZ-CUÉLLAR, N., «Garantías constitucionales en la persecución penal del entorno digital» en Derecho y Justicia penal del siglo XXI. *Liber Amicorum en homensaje al Profesor A. González-Cuéllar García*, Madrid, 2006, pp. 1 y ss.

HYDER, S., «The Fourth Amendment and Goverment Interception of Unsecured Wireless Communications», 28 *Berkely Tech. Law Journal* (2013), pp. 937-962.

JIMÉNEZ SEGADO, C., y PUCHOL AIGUABELLA, M., «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos», *La Ley*, n.º 8676, 7 enero 2016, pp. 1-10.

MARCHENA GÓMEZ, M., y GONZÁLEZ-CUÉLLAR, N., *La reforma de la Ley de Enjuiciamiento Criminal* en 2015, Madrid, 2015.

ORTIZ PRADILLO, J.C., «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica», en J. Pérez Gil (ed.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, Madrid, 2012, pp. 267-310.

RHODEN, C., «Challenging Searches and Seizures of Computers at Home or in the Office: From reasonable Expectation of Privacy to Fruit of the Poisonous Tree Doctrine», 30 *American Criminal Law Journal* (2002-2003), pp. 107-134.

RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», *La Ley,* n.º 8808, 21 julio 2016, pp.1-15.

RUIZ LEGAZPI, A., «Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (*Incoming de eMule*) en la STC 173/2011», REDC núm. 100, enero-abril (2014), pp. 365-390.

SÁNCHEZ NÚÑEZ, T., «La jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal», en *Los nuevos medios de investigación en el proceso penal. Especial referencia a la videovigilancia, CGPJ, Cuadernos de Derecho Judicial,* Madrid 2007, pp. 251-299.

ZOCO ZABALA, C., *Nuevas tecnologías* y *control de las comunicaciones*, Madrid, 2015.