IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos*

Inmaculada López-Barajas Perea
Profesora titular acreditada de Derecho procesal
Universidad Nacional de Educación a Distancia

Fecha de presentación: noviembre de 2016
Fecha de aceptación: enero de 2017
Fecha de publicación: febrero de 2017

Resumen
La lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, es fundamental para garantizar la seguridad y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación. Sin embargo, este objetivo de interés general, aunque sea primordial, no puede justificar por sí solo la existencia de cualquier medida de investigación. En este trabajo, se analizan algunas de las garantías que deben observarse en la intervención de los equipos informáticos atendiendo a las singularidades que esta medida presenta en un entorno digital e interconectado a nivel mundial. Las múltiples funciones y la variada información que se suele almacenar en estos dispositivos exige una especial protección constitucional.

Palabras clave
investigación penal, nuevas tecnologías, derechos fundamentales, intimidad, privacidad, dispositivos de almacenamiento masivo de información, prueba

Tema
investigación tecnológica del delito

* Este trabajo ha sido realizado en el marco del proyecto de investigación concedido por el Ministerio de Economía y Competitividad del Estado español «Retos procesales para afrontar el uso criminal de las TIC en la sociedad de la información», DER2013-47856-P.

New technology applied to criminal investigation: searching computers

Abstract

The fight against serious crime, and in particular against organised crime and terrorism, is of great importance in order to guarantee security, and its efficacy depends very much on the use of modern investigation techniques. However, although this general interest objective is crucial, it cannot justify the use of any kind of investigative measures. In this paper we analyse some of the guarantees that should be observed when searching and tapping into computers, keeping in mind the unique features that this measure presents in a digital world that is interconnected at the world level. The multiple functions of computers and the varied information that is usually stored in them calls for special constitutional protection.

Keywords

criminal investigation, new technologies, human rights, intimacy, privacy, information massive storage devices, evidence

Topic

technological investigation of crimes

1. Proceso penal y nuevas tecnologías

La garantía del derecho a la esfera privada es uno de los grandes desafíos de los ordenamientos jurídicos en la actualidad y, por ende, también de nuestro proceso penal. Este tutela un intenso interés público: la represión jurídica de las conductas criminales. En el ejercicio de esta esencial función del Estado, ha de estar siempre presente la adecuada defensa de los derechos y libertades de las personas implicadas.[1]

Este trabajo tiene por objeto el estudio de la reforma de la normativa procesal penal española de 2015 en relación con las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la constitución y, en concreto, de la diligencia consistente en el registro de los equipos informáticos.

La sociedad que alumbró la Ley de Enjuiciamiento Criminal de 1882 ha experimentado una transformación muy profunda. Actualmente, la informática y las telecomunicaciones son la base tecnológica que gestiona prácticamente todos los ámbitos de nuestra vida diaria.[2] Los modelos de negocio, de ocio e, incluso, la estrategia militar[3] se diseñan con base en la red.[4]

También la delincuencia organizada ha aprovechado los progresos de la ciencia en el ámbito de las telecomunicaciones para ampliar su infraestructura y potenciar la consecución de sus fines ilícitos. Se manifiesta de forma cada vez más violenta y más sofisticada en los medios y técnicas que

1. Gimeno Sendra (2015, pág. 66-68); De la Oliva Santos (2005, pág. 175-199).
2. Llamas Fernández y Gordillo Luque (2007, pág. 207 y ss.).
3. Los avances tecnológicos de los sistemas de información han llevado a algunos autores a definir la guerra de la era de la información como una guerra digital.
4. Exposición de Motivos de la Ley de servicios de la sociedad de la información y comercio electrónico 34/2002; Salom Clonet (2008, pág. 152).
5. Magro Servet (2007).

utiliza, actuando de forma rápida, masiva y continuada.[5] De hecho, casi todas las infracciones penales tienen hoy un soporte tecnológico.

Para poder dar respuesta a las formas de delincuencia ligadas al uso de las nuevas tecnologías, junto a los actos de instrucción «clásicos», han aparecido otros que exigen buscar un adecuado equilibrio entre seguridad y privacidad. De un lado, la capacidad del Estado para hacer frente a esta fenomenología criminal de nuevo cuño.[6] De otro, el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros. Es necesario ponderar despacio la injerencia en la esfera de los derechos fundamentales para que no se desvirtúe su contenido esencial.[7]

Esta tarea se ha visto dificultada porque nuestra Ley de Enjuiciamiento Criminal, ha estado durante mucho tiempo huérfana de regulación con respecto a estos actos de investigación, nacidos con la aparición de las nuevas tecnologías, lo que ha ocasionado no pocos problemas procesales.[8] A ello se une que nos encontramos ante un campo sujeto a la innovación y la evolución casi permanentes que aporta la ciencia y que opera en un entorno virtual e interconectado a nivel mundial.

2. La reforma de la Ley de Enjuiciamiento Criminal

El Tribunal Constitucional ha apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. La falta de previsión legal ha tenido una repercusión muy negativa en la persecución de los delitos. Basta con mencionar la STC145/2014, de 22 de septiembre, que declaró ilegítima la grabación de las conversaciones entre dos personas detenidas efectuadas en la comisaría de policía, por incumplimiento del requisito de reserva de Ley orgánica, aun cuando dichas intervenciones se hubieran realizado con autorización judicial. Se declaró la falta de cobertura legal para acordar una medida de esta naturaleza.

Se afirma la necesidad de una previsión normativa que aporte seguridad y que proporcione claridad en la definición de los límites de la restricción de los derechos fundamentales afectados.

Los dos últimos intentos de reforma global de nuestra centenaria Ley de Enjuiciamiento criminal no se han podido llevar adelante.[9]

Ha sido una nueva modificación parcial de la Ley de Enjuiciamiento Criminal, mediante la Ley orgánica 13/2015, de 5 de octubre, que trata de paliar la situación de insuficiencia normativa en la que se encontraban la mayoría de las medidas de investigación tecnológica. El nuevo título VIII (dentro del capítulo III del libro II), bajo la rúbrica «De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución», regula determinados actos de injerencia que no estaban previstos en la normativa anterior, como la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. Asimismo, se actualiza y se regula la interceptación de las comunicaciones telefónicas y telemáticas, y se confiere sustantividad propia a otras formas de comunicación telemática, como los mensajes SMS y el correo electrónico.

Se establecen unas disposiciones comunes para todas estas medidas de investigación tecnológica que deben satisfacer los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados.

6. Gascón Inchausti (2001, pág. 1-9).
7. Fenwick y Phillipson (2011, pág. 863-918).
8. SSTC 49/1999, de 5 de abril, 184/2003, de 23 de octubre, y 26/2006, de 30 de enero. SSTEDH de 30 de julio de 1988, Valenzuela Contreras contra España, y de 18 de febrero de 2003, Prado Bugallo contra España.
9. Anteproyecto de ley para un nuevo proceso penal. Ministerio de Justicia, Secretaría General Técnica, 2011. DL:M-32828-2011; Borrador de código procesal penal elaborado por la Comisión Institucional para la elaboración de un texto articulado de la Ley de Enjuiciamiento Criminal constituida por acuerdo del Consejo de Ministros de 2 de marzo de 2012.

3. El registro de los dispositivos de almacenamiento masivo de información

Dentro de las nuevas diligencias de investigación, desempeñan un papel destacado, por su relevancia en la instrucción de las causas por delito, el registro y la incautación de la información almacenada en los equipos informáticos (los tradicionales discos duros de los ordenadores) y demás unidades de almacenamiento masivo de información,[10] que se ha convertido en una práctica imprescindible, cuando se lleva a cabo un registro, con el fin de encontrar evidencias digitales del delito investigado.[11] Es relevante como medio de obtención de información, pero también como fuente de prueba.[12]

Según la doctrina, se configura como un acto de prueba preconstituida del juez de instrucción.[13] Conviene recordar que estos actos tienen un carácter asegurador de los indicios o fuentes de prueba, y bajo determinadas garantías formales, de entre las que destaca la posibilidad de contradicción, posibilitan su introducción en el juicio oral, a través de la lectura de documentos, como documentos públicos oficiales suficientes para fundar una sentencia de condena.[14] Se caracterizan por estar predominantemente orientados a la obtención de elementos o datos relacionados con el delito que puedan servir como prueba en el proceso y porque implican, con carácter general, una limitación de ciertos derechos fundamentales.

Los actos de prueba preconstituida tienen una relevancia práctica enorme, ya que la mayoría de las sentencias penales se fundan, sobre todo, en ellos. De ahí que sea necesario que cumplan escrupulosamente unas garantías.

3.1. El registro de dispositivos y derechos fundamentales afectados

Tal y como se ha indicado, la Ley 13/2015, de 5 de octubre, regula por primera vez el «registro de dispositivos de almacenamiento masivo de información», que hasta ese momento se encontraban en una situación de vacío normativo, salvo lo dispuesto en el convenio de Budapest de 2001 sobre ciberdelincuencia.[15]

Hasta la entrada en vigor de esta ley, la legitimidad del acceso a los datos contenidos en estos dispositivos, esto es, el régimen legal para practicar esta diligencia de investigación se había fundado en los preceptos sobre registro de libros y papeles y recogida de otros efectos e instrumentos del delito que siguen estando vigentes, pero agrupados en el nuevo capítulo II, del título VIII del libro II de la Ley de Enjuiciamiento Criminal, bajo la rúbrica «Del registro de libros y papeles». Conforme a dicho régimen, la policía, tras un registro domiciliario, podía intervenir el disco duro de un ordenador. Tras la entrada en vigor de la reforma 13/2015, esta posibilidad queda prohibida por el artículo 588 sexies a.

Según el artículo 575 de la Ley de Enjuiciamiento Criminal, todos están obligados a exhibir los objetos y papeles que se sospeche puedan tener relación con la causa.[16] Por ello, la primera cuestión que se plantea es si los dispositivos de almacenamiento masivo de información son o no efectos e instrumentos del delito. Nos preguntamos si cuando hablamos de objetos o papeles, estos sufren una excepción cuando sean informáticos o tengan un soporte tecnológico.

Se ha defendido que no es posible equiparar las tradicionales cartas, agendas o mochilas que una persona lleva consigo a los actuales dispositivos electrónicos, dada la

10. Van Someren (2007).
11. Urbano Castrillo (2007, pág. 28 y 29).
12. De Jorge Mesas (2007, pág. 358-365).
13. *Cfr.* Gimeno Sendra (2015, pág. 363 y 379).
14. De la Oliva Santos (2005, pág. 119-129).
15. Este convenio, publicado en el BOE de 17 de septiembre de 2010 y en vigor en España desde el 1 de octubre de 2010, prevé expresamente como medida de investigación el registro y decomiso de los datos informáticos almacenados.
16. El artículo 574 de la Ley de Enjuiciamiento Criminal ordena recoger los efectos e instrumentos del delito y también los libros, papeles o cualquiera otra cosa que se hubiesen encontrado, si esto fuere necesario para el resultado del sumario.

cantidad y diversidad de la información almacenable en los mismos.[17] Otra posición, en cambio, entiende que solo cambia el soporte.

Una respuesta a la cuestión planteada exige determinar la intensidad de la injerencia que conlleva esta medida, atendiendo, en primer lugar, a la extensa y variada funcionalidad de tales dispositivos. Como dice la STS 342/2013, de 17 de abril, «la ponderación de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la funcionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser mas adecuado si los mensajes, imágenes, los documentos y, en general, todos los datos [...] se contemplan de forma unitaria».

Asimismo, debe tenerse en cuenta la variedad de información que se suele almacenar en un ordenador personal. Aunque estos datos puedan tacharse de irrelevantes si se consideran aisladamente, analizados en su conjunto permiten configurar un perfil altamente descriptivo de la personalidad de su titular.[18] Por ello, el Tribunal Constitucional, en la sentencia 173/2011, de 7 de noviembre, considera que esta intromisión no solo afecta al ámbito de la intimidad constitucionalmente protegido, sino que puede afectar a la esfera más íntima del ser humano. Dadas las múltiples funciones de almacenamiento de datos como de comunicación con terceros a través de Internet que posee un ordenador personal, el acceso a su contenido también podrá incidir en el derecho al secreto de las comunicaciones (art. 18.3 CE) si lo que resulta desvelado a terceros son datos relativos a la comunicación.

De conformidad con lo expuesto, el registro y análisis de la información contenida en estos dispositivos presenta algunas singularidades en el entorno digital que los hace dignos de una especial protección constitucional. Los tradicionales amparos a través de la protección del domicilio, la tutela formal del secreto de las comunicaciones o material de la intimidad podrían resultar insuficientes, por lo que sería necesaria una tutela más amplia.[19]

Por su parte, la sentencia de la Sala Segunda del Tribunal Supremo de 17 de abril de 2013[20] considera que existe un derecho al propio entorno virtual. "En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Por ello, todos estos documentos, imágenes, mensajes y datos almacenados deben ser tratados de forma unitaria, de manera que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal.

Como consecuencia, concluye el órgano jurisdiccional superior, la intervención y acceso al contenido de un ordenador exige una autorización judicial específica que no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la intervención del dispositivo en orden a realizar el correspondiente juicio de proporcionalidad.[21]

3.2. La garantía jurisdiccional de la intervención y su contenido

En congruencia con lo expuesto, la Ley 13/2015 de 5 de octubre, de modificación parcial de la Ley de Enjuiciamiento Criminal, afirma que los dispositivos de almacenamiento de

17. Ortiz Pradillo (2012, pág. 305-310).
18. En esta línea, la STEDH, de 3 de abril de 2007, caso Copland contra el Reino Unido, considera que están incluidos en el ámbito de protección del artículo 8 del Convenio europeo, por cuanto pueden contener datos sensibles que afecten a la intimidad, la información derivada del seguimiento del uso personal de Internet.
19. González-Cuellar Serrano (2006, pág. 890).
20. ROJ: STS 2222/2013, de 17 de abril.
21. En el mismo sentido se pronuncian las SSTS 985/2009 de 13 de diciembre, 342/2013 de 17 de abril, 587/2014 de 18 de julio y 97/2015 de 24 de febrero.

información son algo más que simples piezas de convicción. Se exige una autorización judicial motivada e individualizada que justifique las razones de su intervención.

La simple incautación de los dispositivos, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.[22] Se pone así fin a una práctica jurisprudencial que hacía extensiva la autorización judicial concedida para la intromisión en el domicilio a la aprensión de todos los soportes informáticos que pudieran encontrarse en el interior del mismo.[23]

El legislador quiere que la restricción de cada uno de los derechos afectados sea ponderada individualmente por el órgano jurisdiccional que ha de exteriorizar las razones de su sacrificio.[24] Por ello, la necesidad de esa autorización judicial se hace extensiva a los casos en que la aprehensión de estos dispositivos electrónicos se lleve a cabo fuera del domicilio del investigado.[25]

De esta forma, como primera conclusión, a la hora de determinar el régimen jurídico que debe informar la intervención y acceso a los datos contenidos en estos dispositivos, el legislador se ha manifestado restrictivo al exigir que se solicite siempre la correspondiente autorización judicial. Se establece un principio de reserva jurisdiccional del juez de instrucción competente aun cuando la intervención de tales informaciones no siempre limite de facto, como hemos visto, el derecho al secreto de las comunicaciones del artículo 18.3 CE, al poder resultar afectado el derecho a la intimidad y, en cualquier caso, el de la privacidad del artículo 18.1. CE. Queda superada la jurisprudencia que consideraba legítimo el acceso a la memoria del teléfono móvil por los agentes de policía cuando no hubiera un proceso de comunicación en marcha.[26]

No obstante, el rigor de esta exigencia se modula, en los casos de urgencia, en que haya un interés constitucional legítimo que haga imprescindible la medida, en cuyo caso se podrá hacer un examen directo por la policía judicial de los datos, dando cuenta inmediata a la autoridad judicial.[27] Lo mismo ocurre cuando se trate de ampliar el registro a otro sistema informático.

La norma no precisa cómo se determina la urgencia del caso. Tampoco especifica cuándo concurre un interés constitucional legítimo. Si tenemos en cuenta que el Tribunal Constitucional ha venido sosteniendo que reviste esta naturaleza «el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal»,[28] podemos afirmar que se entenderá cumplido este requisito por el mero interés en la persecución y castigo del delito que se está investigando. La Ley no limita el ámbito objetivo de esta medida

22. Artículo 588 sexies a.2 de la Ley de Enjuiciamiento Criminal.
23. La STS 2809/2008, de 14 de mayo, entendió que la orden de entrada y registro habilitaba a la policía para la incautación, entre otras cosas, del material informático que pudiera encontrarse. Por su parte, la STS 4745/2002, 27 de junio, admitió como lícita la lectura de un mensaje grabado en un móvil por considerar que se encontraba bajo la cobertura de la autorización judicial de la entrada y registro. Entendió que los requisitos de validez no eran los propios de una intervención de comunicaciones, sino los que rigen el hallazgo de documentos ya en poder del destinatario.
24. Marchena Gómez y González-Cuellar Serrano (2015, pág. 373).
25. El artículo 588 sexies b dispone que «la exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si este considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización».
26. La STS de 25 de febrero de 2003 recuerda que nuestra jurisprudencia ha afirmado la legitimidad de la indagación en la memoria del aparato móvil de telefonía (SSTS de 27 de junio de 2002 y 25 de julio de 2003), en la que equipara la agenda electrónica del aparato de telefonía con cualquier otra agenda en la que el titular puede guardar números de teléfono y anotaciones sobre las llamadas realizadas y otras anotaciones que indudablemente pertenecen al ámbito de la intimidad, constitucionalmente protegida, y que admiten injerencias en los términos exigidos por el artículo 8 del CEDH y la Constitución, «pues no tiene la consideración de teléfono en funciones de transmisión del pensamiento dentro de una relación privada entre dos personas». Posteriormente, el examen de las llamadas entrantes y salientes fue puesto en cuestión por las SSTS de 8 de abril y 14 de mayo de 2008 y de 18 de diciembre de 2009.
27. Artículo 588 sexies c, apartado 4.
28. SSTC 25/2005, de 14 de febrero, y 206/2007, de 24 de septiembre.

de investigación.[29] La amplitud de la excepción legal choca con la intensidad de la injerencia, dados los derechos fundamentales eventualmente afectados, tal y como ha puesto de manifiesto la jurisprudencia y, más en concreto, presenta dificultades en el caso de contenidos vinculados al derecho a la inviolabilidad de las comunicaciones.

Además, el estado actual de la tecnología debería permitir dar una respuesta inmediata a estas solicitudes de intervención por parte de los jueces de guardia, una de cuyas funciones es, precisamente, actuar en dichas circunstancias,[30] debiendo quedar limitada la excepción a los supuestos excepcionales expresamente previstos.[31]

Para ilustrar la cuestión que nos ocupa, puede servir de ejemplo el supuesto analizado por el Tribunal Constitucional en la sentencia 173/2011. Un técnico de mantenimiento informático recibió el encargó de reparar el micrófono de un ordenador. Una vez hecha la reparación, con el fin de comprobar el correcto funcionamiento de las piezas (según el protocolo habitual), el técnico eligió al azar diversos archivos para su grabación y posterior reproducción, para lo cual accedió a la carpeta llamada «mis documentos/mis imágenes» del ordenador, encontrando diversos archivos fotográficos de contenido pedófilo. Denunció inmediatamente los hechos y la policía procedió a la comprobación del disco duro sin solicitar la correspondiente autorización judicial. Tras analizar el caso, el TC concluyó que la actuación policial fue legítima, pues el sacrificio del derecho fundamental afectado estaba justificado por la presencia de otros intereses constitucionalmente relevantes.[32] El TC valoró la conveniencia de que se actuara con rapidez para evitar la destrucción de archivos y comprobar la posible existencia de otros partícipes. También tuvo en cuenta la gravedad de estos hechos, por afectar a menores de edad, esto es, a víctimas especialmente vulnerables. Se trataba de un caso de distribución de pornografía infantil en el que se utilizó una aplicación informática que permitía el intercambio de archivos.

Por último, conviene poner de manifiesto que la ley también omite que el consentimiento inequívoco del usuario actúa como verdadera fuente de legitimación, tal y como ha establecido la jurisprudencia.[33] Corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, por lo que el consentimiento del titular del derecho fundamental legitimará la intromisión en el ámbito de la intimidad e impedirá, por tanto, considerarlo vulnerado. La persona afectada deberá ser informada adecuadamente sobre la diligencia para la cual presta consentimiento y sobre su finalidad.[34] Se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto, aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida.[35]

3.3. Objeto del registro

El artículo 588 sexies a de la Ley de Enjuiciamiento Criminal se refiere a la aprehensión de ordenadores, instrumentos

29. En el caso analizado en la STC 115/2013, de 9 de mayo, la urgencia de la intervención resultó de la necesidad de averiguar la identidad de las personas que escaparon al ser sorprendidas *in fraganti* custodiando droga, para proceder a su detención e impedir que se sustrajeran definitivamente a la acción de la justicia.
30. STEDH, de 2 de diciembre de 2014, Taraneks contra Letonia.
31. Enmiendas presentadas en este punto durante la tramitación del proyecto de Ley orgánica de 13 de marzo de 2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.
32. La policía puede realizar injerencias en el derecho a la intimidad de carácter leve, siempre que se respeten los presupuestos derivados del principio de proporcionalidad. La STC 115/2013, de 9 de mayo, permite que en algunos casos y con la suficiente y precisa habilitación legal, la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, STC 70/2002, de 3 de abril).
33. *Cfr.* STS 97/2015, de 24 de febrero. En lo relativo a la forma de prestación del consentimiento, el Tribunal Constitucional ha manifestado que este no precisa ser expreso, admitiéndose también un consentimiento tácito, derivado de la realización de actos concluyentes que expresen dicha voluntad. La mera falta de oposición a la intromisión no podrá entenderse como un consentimiento tácito (SSTC 22/1984, de 17 de febrero, y 209/2007, de 24 de septiembre, respecto a la entrada en un registro domiciliario).
34. STC 206/2007, de 24 de septiembre.
35. SSTC 196/2004, de 15 de noviembre, 206/2007, de 24 de septiembre, y 70/2009, de 23 de marzo.

de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital y de acceso a repositorios telemáticos de datos.

Se trata de un concepto amplio que está sujeto a la evolución propia de los sistemas de comunicación.[36] Abarca todos aquellos instrumentos que incluyen entre sus funcionalidades la de servir de soporte para el almacenamiento masivo de datos.

Sin embargo, a la hora de determinar el objeto de esta medida, lo que resulta fundamental es tener en cuenta la deslocalización de la información digital. Los datos pueden guardarse no solo en dispositivos físicos, que podemos tocar y aprehender, sino también en dispositivos en la nube, alojados en servidores situados a distancia del usuario mediante las técnicas de computación en la nube o *cloud computing*. De esta manera, se puede acceder a los datos desde el domicilio a través del dispositivo investigado, pero eso no implica que la información esté localizada en dicho lugar.[37]

Así, el dispositivo en sí mismo presenta menor relevancia, salvo en aquellos casos en que el objeto sobre el que haya recaído el delito sea el propio dispositivo o equipo. Lo que de verdad importa es la información contenida en sus archivos.[38] El soporte es únicamente el medio a través del cual la información será emitida o preservada.[39]

En un entorno digital e interconectado a nivel mundial es necesario determinar el ámbito al que se extiende el registro de estos dispositivos cuando están interconectados a la red.

Por eso, el Convenio sobre la Ciberdelincuencia, elaborado en Budapest el 23 de noviembre de 2001, entiende que el sistema informático no es solo el dispositivo aislado en cuestión, sino también el conjunto de dispositivos interconectados o relacionados entre sí, que permiten, en la ejecución de un programa, el tratamiento automatizado de datos.

El mencionado Convenio permite ampliar, con ciertas limitaciones, el registro a otros sistemas informáticos cuando existan motivos para pensar que los datos buscados se hallen allí almacenados. Se exige siempre que esos sistemas se encuentren en el territorio español y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para este. También se permite el acceso transfronterizo a los datos almacenados, pero solo cuando se trate de datos de libre acceso al público o con el consentimiento lícito y voluntario de la persona legalmente autorizada para divulgarlos a través de ese sistema informático.

Fuera de estos supuestos, la autoridad investigadora debe remitir la correspondiente solicitud de asistencia judicial internacional. Esta petición puede fundamentarse en el propio Convenio de Budapest o bien en otro tratado o instrumento internacional que resulte aplicable. Resulta imprescindible prever nuevos instrumentos de cooperación internacional que contemplen estas nuevas medidas de investigación y permitan una respuesta rápida a las solicitudes de cooperación judicial y policial entre los distintos países con el fin de encontrar evidencias digitales del delito en la línea de lo establecido por la Recomendación R (95) 13, del Comité de Ministros del Consejo de Europa, de 11 de septiembre, relativa a los problemas de la legislación procesal penal conectados con las tecnologías de la información.

Mediante la reforma de la Ley de Enjuiciamiento Criminal llevada a cabo por la LO 13/2015, de 5 de octubre, se prevé, por primera vez en nuestro Derecho, la posibilidad de extender el registro a otros sistemas conectados con el originariamente investigado. Así, el nuevo artículo 588 sexies 3.c permite la ampliación del registro cuando se tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. En estos casos, se impone una nueva autorización judicial que pondere la necesidad de esa ampliación. No obstante, en caso de urgencia, la policía judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente y, en todo caso, dentro del plazo de veinticuatro horas, de la actuación realizada, de su forma y de su resultado. El juez

36. Incluye las tabletas, ordenadores, dispositivos USB, ZIP, CD-ROM, DVD, reproductores de MP3 o MP4, y servidores informáticos cuya enumeración no puede agotarse aquí.
37. González-Cuellar Serrano (2006).
38. De Jorge Mesas (2007, pág. 359).
39. Gudín Rodríguez-Magariños (2014).

competente revocará o confirmará la actuación en el plazo de setenta y dos horas.[40]

Procede poner de manifiesto que la ley española guarda silencio sobre la posibilidad de que la medida recaiga sobre sistemas informáticos no ubicados en el territorio español.

Por último, podemos citar las SSTS de 17 de abril de 2013 y de 24 febrero de 2015 (n.º 97/2015), según las cuales el auto judicial por el que se decreta el volcado de datos informáticos contenidos en los ordenadores incautados no permite sin más el acceso a los contenidos de las redes sociales, sino que es preciso acceder a Internet e introducir una clave de usuario, por lo que el apoderamiento del contenido de las redes sociales no se obtiene simplemente por el acceso al contenido del ordenador, sino que se requiere una acción adicional dirigida expresamente a su apertura y examen, siendo necesario el dictado de un nuevo mandamiento judicial.

3.4. Ejecución

La ley se limita a decir que la resolución del juez de instrucción fijará los términos y el alcance del registro, y las cautelas necesarias para asegurar la integridad de los datos. No obstante, la ley exige el cumplimiento del principio de la alternativa menos gravosa. Así, salvo en el caso de que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se intentará evitar la incautación de los soportes físicos, cuando ello pueda causar un grave perjuicio al titular, y se obtendrá una copia.[41]

De esta manera, los dispositivos podrán seguir siendo utilizados por sus usuarios. Además, dada la inmediatez entre la intervención de la información y su volcado, se gana en eficacia de la evidencia digital, que queda garantizada en el acto de la entrada y registro.

Como todas las piezas de convicción, es necesario asegurar la autenticidad e integridad de la información obtenida. El 588 sexies c.1 de la Ley de Enjuiciamiento Criminal, se limita a disponer que corresponde al juez fijar las condiciones necesarias para asegurar y preservar los datos que deben acceder al proceso en el mismo estado en el que fueron obtenidos, sin alteraciones ni manipulaciones.[42]

Ahora bien, la información digital presenta algunas peculiaridades respecto a la información en papel, por lo que no pueden aplicarse los métodos clásicos de documentoscopia. Teniendo en cuenta que el juez no es un técnico en la materia, resulta necesario que su actuación venga apoyada y complementada por conocimientos especializados que aseguren que el volcado o la copia de seguridad se han efectuado con las garantías de autenticidad e integridad.[43]

El análisis de los datos contenidos en el dispositivo intervenido puede requerir la realización de actuaciones complejas, como la recuperación de archivos borrados u operaciones de desencriptado, que exigen conocimientos especializados, programas específicos y la última tecnología.[44]

La ejecución de la medida corresponde a la policía judicial, que puede ordenar a cualquier persona experta que conozca el funcionamiento del sistema informático o las medidas tomadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no se derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.[45] Esta disposición no será aplicable al investigado o encausado, a las personas que están dispen-

40. La enmienda número 38 establece que el prelegislador no explica los motivos que justifican el establecimiento de un plazo distinto y mayor (de setenta y dos horas) que en los demás supuestos análogos previstos en la reforma del título VIII para obtener la resolución judicial (veinticuatro horas), por tanto, parece más adecuado homogeneizar su tratamiento.
41. El artículo 588 sexies a, apartado 2 dispone que «salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos».
42. El artículo 338 de la Ley de Enjuiciamiento Criminal dispone que «sin perjuicio de lo establecido en el capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el juez acordará su retención, conservación o envío al organismo adecuado para su depósito».
43. Urbano Castrillo (2007, pág. 57); De Jorge Mesas (2007, pág. 365).
44. Fernández Lázaro y Gordillo Luque (*op. cit.*, pág. 141 y ss).
45. Artículo 588 sexies c, apartado 5 de la Ley de Enjuiciamento Criminal.

sadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional, entre las que se encuentra el abogado defensor.

Sin perjuicio de lo expuesto, debe llamarse la atención sobre la necesidad de que los jueces y fiscales reciban una formación permanente sobre estas cuestiones para que puedan tomar las decisiones que les competen y no acepten a ciegas la opinión de los expertos.[46]

Aunque la ley no dice nada expresamente, es necesario documentar estos registros. El letrado de la Administración de justicia deberá levantar acta detallada en la que consten las operaciones practicadas y las personas intervinientes.

En cuanto a la presencia del fedatario judicial en las operaciones técnicas de volcado, la jurisprudencia ha matizado que su intervención no constituye un presupuesto de validez, toda vez que se trata de un proceso extremadamente complejo e incomprensible para un profano, pues consiste en el análisis y desentrañamiento de los datos incorporados a un sistema informático. A juicio de esta jurisprudencia, ninguna garantía podría añadirse con la presencia del letrado de la Administración de justicia, al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia. Su presencia sería, de facto, inútil y, por tanto, innecesaria, pues se trata de una técnica en la que el fedatario judicial no es un experto (STS 256/2008, de 14 de mayo). Lo decisivo es que, ya sea mediante la intervención de aquel durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado (STS 480/2009, de 22 de mayo).

Las partes tienen derecho a estar presentes en las actuaciones que implican una preconstitución de prueba, como parte del derecho de contradicción.[47] Se les debe dar la posibilidad de estar presentes con el fin de que puedan conocer las circunstancias de la intervención y acceso a los dispositivos y manifestar, en su caso, lo que tenga por conveniente sobre la forma en la que estas operaciones se han llevado a cabo.

Asimismo, debe quedar identificado el lugar donde fueron obtenidos los soportes informáticos o dispositivos de almacenamiento de datos,[48] que se custodiarán en lugar adecuado para evitar su perdida y manipulación.[49]

También faltan en la ley normas que habiliten a la policía para tomar medidas con el fin de evitar el alzamiento o autodestrucción de los datos, medidas que resultan determinantes para el éxito del registro.

Finalmente, la intervención de las referidas informaciones, efectuadas con todas las garantías, y las pericias efectuadas sobre ellas tendrán el valor de prueba preconstituida, que, no obstante, podrá ser impugnada en el juicio oral a través de la pericial correspondiente.

4. Conclusiones

Debe hacerse una valoración general positiva de la reforma, en cuanto que nuestro Derecho está necesitado de una regulación de las medidas de investigación tecnológica que se adapte a los tiempos en que vivimos y que cumpla con las exigencias de la existencia de una norma legal habilitante para la restricción de los derechos fundamentales. No se puede justificar la utilización de ciertos medios de investigación sin una mínima base legal que regule sus requisitos y límites.[50]

46. Verdelho (2009).
47. Abel Lluch (2013, pág. 194).
48. La STC 170/2003, de 29 de septiembre, declaró la vulneración del derecho a un proceso con todas las garantías por falta de las garantías procesales exigibles en la incorporación del material al proceso. Al no identificarse el domicilio (de los varios registros que se habían practicado) en que habían sido recogidos unos soportes informáticos, ni haberse procedido al sellado ni precintado de dichos soportes, entiende que la recogida de las piezas de convicción y su custodia fue irregular.
49. Urbano Castrillo (2007, pág. 66); Frings (2007).
50. De esta manera, se da cumpliendo a las obligaciones derivadas de la ratificación del Convenio de Budapest sobre Ciberdelincuencia del 23 de noviembre de 2011, cuyo artículo 19 establece que cada parte adoptará las medidas legislativas y de otro tipo para facultar a las autoridades competentes a registrar o a tener acceso de forma similar a un sistema informático o a medios de almacenamiento de datos informáticos.

Asimismo, la nueva regulación permite superar la disparidad de criterios que, en numerosos aspectos, refleja la jurisprudencia de nuestros tribunales.

Desde este punto de vista, se trata de un paso indudable en la actualización de nuestro proceso penal que anuncia parte del futuro por donde este discurrirá.

Ahora bien, resulta necesario seguir avanzando para conseguir un adecuado equilibrio entre seguridad y privacidad en la investigación penal del delito, lo que constituye un reto permanente como consecuencia de la evolución constante de la ciencia en el ámbito de las telecomunicaciones.

La vida privada es un término abierto no susceptible de una definición exhaustiva que, según el Tribunal Europeo de Derechos Humanos, debe ser interpretado a la luz de las condiciones actuales de vida propias de la sociedad de la información en la que estamos inmersos para proteger al individuo de forma real y efectiva en aquellos ámbitos a los que se refiere.

Desde esta perspectiva, la nueva ley adolece de algunas insuficiencias, tal y como se ha puesto de manifiesto en este trabajo, respecto al registro de los equipos informáticos.

Asimismo, para conseguir un proceso penal eficaz en una sociedad globalizada, también resulta imprescindible prever nuevos instrumentos de cooperación internacional que contemplen estas nuevas medidas de investigación y que permitan dar una respuesta rápida a las solicitudes de cooperación judicial y policial entre los distintos países con el fin de encontrar evidencias digitales del delito.

Referencias bibliográficas

ABEL LLUCH, X. (2013). «Nuevas tecnologías e investigación penal». En: VV. AA. *Estudios sobre prueba penal, III*. Madrid: La ley.

BRENNER, S. (2007). «At light speed: attribution and response to cybercrime, terrorism, Warfare». *Journal of Criminal Law & Criminology*. N.º 97.

BUENO DE LA MATA, F. (2015). *FODERTICS 4.0*. Granada: Comares.

DE JORGE MESAS, L. F. (2007). «La incorporación de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal (...más sobre las nuevas tecnologías)». En: *Nuevos medios de investigación en el proceso penal*. Cuadernos de Derecho Judicial, CGPJ.

DE LA OLIVA SANTOS, A. (2005). «Consideraciones procesales sobre documentos electrónicos y firma electrónica». *Revista Crítica de Derecho Inmobiliario*. N.º 687.

FENWICK, H.; PHILLIPSON G. (2011). «Covert derogations and judicial deference: redefining liberty and due process rights in counterterrorism Law and beyond». *McGill LJ-RD McGill*. Vol. 56, n.º 4, pág. 863-918. <https://doi.org/10.7202/1005848ar>

FRINGS, S. (2007). «Método de documentación estructurada para la gestión de incidencias de TI». *e-Newsletter, Cyvex*. Abril.

GASCÓN INCHAUSTI, F. (2001). *Infiltración policial y agente encubierto*. Granada: Comares.

GIMENO SENDRA, V. (2015). *Derecho Procesal Penal*. Civitas.

GONZÁLEZ-CUELLAR SERRANO, N. (2006). «Garantías constitucionales en la persecución penal en el entorno digital». En: *Derecho y justicia penal en el siglo XXI*. Líber Amicorum *en homenaje al Prof. Antonio González-Cuellar García*. Colex.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E. (2014). «Incorporación al proceso del material informático intervenido durante la investigación penal». *Boletín del Ministerio de Justicia*. N.º 2163.

LLAMAS FERNÁNDEZ, M.; GORDILLO LUQUE, J. M. (2007). «Medios técnicos de vigilancia». En: *Nuevos medios de investigación en el proceso penal*. Cuadernos de Derecho Judicial, CGPJ.

MAGRO SERVET (2007). «Intervención policial de mensajes SMS y eficacia de las juntas provinciales de Policía Judicial». *Diario La Ley*, N.º 6764.

MARTÍN MORALES, R. (2015). *El régimen constitucional del seguimiento directo de personas.* Granada: Comares.

MARCHENA GÓMEZ, M.; GONZÁLEZ-CUELLAR SERRANO, N. (2015). *La reforma de la Ley de Enjuiciamiento Criminal de 2015.* Madrid: Castillo de Luna.

MEESTER, KAREL DE (2015). *The investigation phase in international criminal procedure. In search of common rules*. Cambridge, U. K.: Intersentia Ltd.

ORTIZ PRADILLO, J. C. (2012). «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica». En: *El proceso penal en la sociedad de la información.* Madrid: La Ley.

SALOM CLONET, J. (2008). «Incidencia de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos». En: VV. AA. *La protección de datos en la cooperación policial y judicial.* Cizur Menor: Thomson-Aranzadi.

URBANO CASTRILLO (2007). «La investigación tecnológica del delito». En: *Nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia.* Cuadernos de Derecho Judicial, CGPJ.

VAN SOMEREN, N. (2007). *Accessing Digital Evidence and RIPA*. Part III. Hutton, U. K.: Credit Control, House of Words, Ltd.

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

VELASCO NÚÑEZ (2016). *Delitos tecnológicos: definición, investigación y prueba en el proceso penal.* Sepin.

VELASCO SAN MARTÍN, C. (2016). *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*. Valencia: Tirant lo Blanch.

VERDELHO, P. (2009). «La cibercriminalidad y las pruebas electrónicas». *e-Newsletter en la Lucha Contra el Crimen.* N.º 1, julio.

Cita recomendada

LÓPEZ-BARAJAS PEREA, Inmaculada (2017). «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos». *IDP. Revista de Internet, Derecho y Política*. N.º 24, págs. 64-76. UOC [Fecha de consulta: dd/mm/2017]. <http://dx.doi.org/10.7238/idp.v0i24.3084>

Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (IDP. *Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: http://creativecommons.org/licenses/by-nd/3.0/es/deed.es.

Sobre la autora

Inmaculada López-Barajas Perea
ilopezbarajas@der.uned.es

Profesora titular acreditada de Derecho Procesal
Universidad Nacional de Educación a Distancia

<http://portal.uned.es/portal/page?_pageid=93,40318578&_dad=portal&_schema=PORTAL>

UNED, Facultad de Derecho
Calle Obispo Trejo 2
28040 Madrid