EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

The search and seizure of mass storage devices

Francisco de Paula Sánchez Medrano
ABOGADO
franciscosanchez@bufetebaenabocanegra.com

Palabras clave: Registro de dispositivos. Autorización judicial para búsqueda e incautación. Almacenamiento masivo. Garantías procesales. Integridad de los datos.
Keywords: device examination, search and seizure warrant, mass storage, procedural guarantees, data integrity.

Resumen: El registro de dispositivos de almacenamiento masivo de información es en la actualidad una herramienta de gran utilidad para la investigación de delitos dada la gran cantidad de datos que estos albergan. Dada la incidencia de esta medida sobre los derechos fundamentales del investigado, en el año 2015 esta fue regulada partiendo del marco jurisprudencial previo, pero por desgracia algunos aspectos no han sido desarrollados por esta nueva normativa. En el presente artículo se exponen los principales aspectos relacionados con esta medida de investigación, su control judicial y la forma de incorporar los resultados al procedimiento.
Abstract: The search and seizure of mass storage devices is currently a very useful tool for crime investigations given the large amount of data hosted. Given the incidence of this measure on the fundamental rights of the defendant, in 2015 it was regulated based on the settled case-law, but unfortunately some aspects have not been developed by this new regulation. This paper exposes the main aspects related to this investigative measure, its judicial control and how to incorporate the results into the procedure.

I. INTRODUCCIÓN

La Revolución Digital, que comenzó en la segunda mitad del siglo XX y que aún continúa, no ha dejado ámbito social ni vital a salvo de transformaciones, resultando innecesario e imposible enumerar todas las funciones que pueden ser realizadas en la actualidad con un ordenador, un *smartphone* o una tableta, lo que ha llevado a que estos equipos sean indispensables en todos los ámbitos de nuestras vidas.

La posibilidad de que con un solo dispositivo se pueda tener acceso a la mayor biblioteca del mundo, llevar toda la gestión de una empresa, mantener el contacto con amigos y familiares, captar y almacenar fotografías y vídeos, y un largo etcétera, lleva también a que, a través del análisis de ese mismo dispositivo, se pueda averiguar todo —o casi todo, puede que lo más secreto— de una persona, ocurriendo lo mismo con el análisis de dispositivos destinados a ser contenedores de la información que los equipos tecnológicos generan.

La Constitución Española, ya en el año 1978, preveía que la informática llegaría a un nivel de desarrollo tal que necesitaría del establecimiento de limitaciones legales a su uso para garantizar la protección de los derechos fundamentales de los ciudadanos[1], aunque quizá no podía prever el grado de desarrollo actual y su incidencia en la vida cotidiana.

La CE diseña mecanismos de protección de derechos fundamentales que difieren en su articulación dependiendo de cuál sea el que se vea afectado, pero que presentan un núcleo esencial común de protección cuando su limitación se produce por parte de una autoridad pública (principio de proporcionalidad, en sentido amplio), quizá sin prever del todo que el desarrollo tecnológico llevase a la afectación de varios de ellos de una sola vez; piénsese en cuáles son los derechos fundamentales susceptibles de verse afectados con la incautación de un *smartphone* y el posterior análisis de su contenido en el momento actual en el que nos encontramos, donde un teléfono móvil es, queramos o no, una extensión de nosotros mismos.

En el registro de dispositivos que se mencionaban en el párrafo anterior es difícil imaginar un caso en el que no se afecte al mismo tiempo al derecho a la intimidad y al secreto de las comunicaciones, aunque pueden ser otros los que se vean afectados llegado el caso. En el escenario actual, tal como apunta la STS 246/2014, de 2 de abril (F.J. 5º), «son muchos los espacios de exclusión que deben ser garantizados» y «[n]o todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional».

Señala Pérez Estrada que «[e]l TC ha intentado describir el contenido de cada derecho fundamental atendiendo a los datos individualmente considerados pero esta tarea cede ante el cúmulo de datos contenidos en los dispositivos de almacenamiento que hace que resulte imposible identificar de manera aislada los derechos fundamentales implicados, pues, muchas veces, aparecen entremezclados»[2], teniendo un ejemplo de ello en la STC 173/2011, de 7 de noviembre[3], de referencia sobre esta materia, que ha sido muy criticada[4]. En dicha sentencia el Tribunal Constitucional advertía de que a través de los datos contenidos en un ordenador personal se puede llegar a descifrar lo más íntimo de una persona, «pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE)», por lo que cualquier registro de dispositivos de almacenamiento masivo de información debe llevarse a cabo previa autorización judicial excepto en el caso de consentimiento del afectado por la medida o de urgente necesidad[5], siempre que la medida sea proporcionada y se persiga un fin legítimo.

No mucho después de la citada STC, el Tribunal Supremo, en la STS 342/2013, de 17 de abril (F.J. 8.º), indicaba que los dispositivos de almacenamiento masivo de información habitualmente contienen «información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones», siendo más adecuado dar un tratamiento unitario a todos los datos que forman parte de ese «entorno virtual»[6] que estaría formado por «toda la información en

1. Artículo 18.4 de la CE:
   «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».
2. Pérez Estrada, «La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información», *Revista Brasileira de Direito Processual Penal*, vol. 5, núm. 3, 2019, p. 1311.
3. Ver los fundamentos de derecho segundo, tercero y cuarto, en los que se mencionan, entre otros derechos susceptibles de ser vulnerados con el análisis de un ordenador, el derecho a la intimidad, al secreto de las comunicaciones y el secreto profesional.
4. Ruiz Legazpi, «Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (*incoming* de *eMule*) en la STC 207/2011», *Revista española de derecho constitucional*, vol. 34, núm. 100, 2014, p. 367.
   «(…) la STC 173/2011 avala una condena por un delito tan grave y deleznable como es la distribución de pornografía infantil, impuesta sobre la base de una prueba ilegal que debió excluirse del proceso, tal como manda la teoría del árbol envenenado plasmada en el artículo 11.1 de la LOPJ, pues se había obtenido quebrantando el derecho a la intimidad del artículo 18.1».
5. En el caso concreto, el propietario de una tienda de informática denunció ante la policía que dentro del ordenador de un cliente había encontrado material pedófilo, les entregó el ordenador a los agentes, facilitó sus datos y lo reconoció fotográficamente; tras esto, los agentes incautaron y visionaron el contenido del ordenador, procediendo luego a la detención del investigado. El TC declara no haber sido vulnerados los derechos fundamentales del propietario del ordenador porque este había consentido la acción del dueño de la tienda de informática, que ante tal hallazgo se encontraba legalmente obligado a denunciar, y la policía había procedido al análisis en una situación de urgente necesidad y persiguiendo un fin legítimo.
   En sentido contrario a la mayoría de la Sala, la Excma. Sra. Dña. Elisa Pérez Vera emitió voto particular señalando, a mi parecer muy acertadamente, que ninguna situación de urgente necesidad podía alegarse pues el investigado estaba detenido y no existía riesgo alguno de borrado de la información porque los ordenadores estaban en poder de los agentes, por lo que perfectamente podía haberse solicitado la autorización judicial antes de proceder al registro.
6. «Entorno virtual» que también es denominado dentro de la misma STS como «*entorno digital*».

ISSN: 2951-844X

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»[7], tratamiento unitario consistente en la necesidad de recabar autorización judicial en todos los casos en los que se pretendiese entrar en el entorno virtual del investigado. Así, como señala Sánchez Gómez[8], es precisamente en base a la multifuncionalidad de los datos y de los soportes en que estos se insertan, como a los derechos susceptibles de ser limitados con su intervención, donde también converge la protección de datos personales y su correlativa protección de la autodeterminación informativa, que debe traerse a colación el derecho a la protección del entorno virtual de las personas. Concepto de creación jurisprudencial donde 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. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital (STS 342/2013, de 17 de abril —F.J. 8.º— y 462/2019, de 14 de octubre —F.J. 1.º—).

Reclamado un tratamiento unitario tanto por la doctrina académica y constitucional como por la jurisprudencia, la Ley Orgánica 13/2015, de 5 de octubre introduce en la Ley de Enjuiciamiento Criminal los artículos 588 sexies a), b) y c) de la LECrim, dentro de unos nuevos capítulos IV a X, insertos en el título VIII del libro II de la LECrim, destinado a la regulación de las medidas de investigación tecnológica, con los artículos 588 bis a) de la LECrim hasta el 588 bis k) de la LECrim a modo de disposiciones comunes. De estas disposiciones comunes, quizá lo más destacable es que el legislador ha decidido introducir dentro del texto legal los principios que el Tribunal Constitucional venía declarando «como determinantes de la validez del acto de injerencia» y del contenido mínimo que debe incluir tanto el oficio policial en el que se solicite la medida como la resolución judicial que la autorice a fin de evitar déficits motivacionales que puedan determinar la posterior declaración de nulidad de la autorización, según el preámbulo de la Ley Orgánica 13/2015, de 5 de octubre[9].

Como veremos más adelante, la normativa introducida por el legislador de 2015 parte del supuesto general de la necesidad de recabar autorización judicial para realizar el registro y el supuesto excepcional de los registros directos por razones de urgencia, dando cuenta posterior al Juzgado y sometido a ratificación, a ello debe sumarse la posibilidad no prevista en la norma de que sea el propio investigado quien consienta la medida, con expresa mención a las

7. Importantísimo el apunte realizado al definir el concepto de entorno virtual, pues en los dispositivos que utilizamos no solamente queda almacenada la información que generamos de forma consciente y voluntaria, sino también la creada a consecuencia del uso dado al dispositivo y que se mantiene oculta, en muchos casos incluso sin saber de la existencia de esta.

8. Sánchez Gómez, «La investigación tecnológica multinivel del discurso terrorista», en *La represión y persecución penal del discurso terrorista* (Galán Muñoz, dir., Gómez Rivero, dir.), Tirant lo Blanch, 2022, pág. 783. Sobre el tratamiento procesal del derecho de configuración jurisprudencial puede consultarse Delgado Martín, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por la LO 13/2015», en *Diario La Ley*, 2016, núm. 8693, pág. 12 y ss., Gómez Colomer, J. L., «Los actos de investigación garantizados», en *Derecho Jurisdiccional III. Procesal Penal* (con Montero Aroca, Esparza Leibar, Barona Vilar, Etxeberría Guridi), Tirant Lo Blanch, Valencia, 2016, págs. 262 y ss. o Gudín Rodríguez-Magariños, A., «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información», *La ley penal: revista de derecho penal, procesal y penitenciario*, 2017, núm. 125, págs. 16 y ss.

9. Párrafos cuarto y quinto del apartado IV del preámbulo de la Ley Orgánica 13/2015, de 5 de octubre:
«*Se ha estimado oportuna la proclamación normativa de los principios que el Tribunal Constitucional ha definido como determinantes de la validez del acto de injerencia. Toda medida deberá responder al principio de especialidad. Ello exige que la actuación de que se trate tenga por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose pues las medidas de investigación tecnológica de naturaleza prospectiva, de acuerdo con el concepto que informa la doctrina emanada del máximo intérprete de la Constitución, por todas la sentencia 253/2006, de 11 de septiembre. Las medidas de investigación tecnológica deben además satisfacer los principios de 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.*
La reforma ha considerado adecuado no abandonar los aspectos formales de la solicitud y del contenido de la resolución judicial habilitante. La práctica forense no es ajena a casos de solicitudes policiales y de ulteriores resoluciones judiciales que adolecen de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación. A evitar ese efecto se orienta la minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial que, en su caso, habilite la medida de injerencia. Las disposiciones comunes se extienden igualmente a las demás cuestiones de forma, tales como la solicitud de prórroga, las reglas generales de duración, el secreto, el control de la medida, la afectación a terceras personas, la utilización de información en procedimiento distinto, el cese de la medida o la destrucción de registros. Cada diligencia modulará algunos de estos aspectos y se regirá por reglas específicas propias de su propia particularidad».

condiciones de validez del consentimiento. Advertir también que aunque el Capítulo VIII se titule «Registro remoto de dispositivos de almacenamiento masivo de información», el artículo 588 sexies a LECrim incluye en su regulación tanto a los equipos que generan los datos como a los de su almacenamiento, incluyendo en su listado ordenadores, instrumentos de comunicación telefónica, telemática, dispositivos de almacenamiento masivo de información digital y repositorios telemáticos de datos.

II. LA AUTORIZACIÓN JUDICIAL HABILITANTE.

1. Principios que informan la resolución habilitante

Como se mencionaba anteriormente, dentro de la nueva regulación existe una serie de disposiciones comunes las nuevas medidas de investigación tecnológicas introducidas por la LO 13/2015, de 5 de octubre, de las cuales quizá la más importante es la positivización de los principios que venía recogiendo el Tribunal Constitucional en sus sentencias para determinar la validez de la injerencia.

Así, el art. 588 bis a.1 de la LECrim dispone que las medidas de investigación tecnológicas gozarán de validez «siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida»; los distintos numerales del mencionado artículo indican el límite que marca cada uno de los principios, si bien no realizan una definición conceptual sobre cada uno de ellos:

a) **El principio de especialidad.**

Según la norma, el principio de especialidad «exige que una medida esté relacionada con la investigación de un delito concreto», no pudiendo autorizarse las medidas «que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva». Debe delimitarse objetivamente la medida a través de la precisión del hecho que se trata de investigar y subjetivamente mediante la suficiente identificación del sospechoso (…)[10]», delimitación objetiva y subjetiva referida al delito investigado, no a la medida interesada en sí, que será valorada atendiendo al principio de idoneidad.

Es doctrina consolidada aquella que proclama que las conocidas como *fishing expeditions* son contrarias a nuestro texto constitucional y que toda investigación que se realice debe partir de la investigación de un delito concreto, no siendo admisible que sea la propia vida de una persona el objeto de la investigación.

El hecho de que solamente se pueda autorizar el registro de dispositivos de almacenamiento masivo durante la investigación de un delito concreto no significa que el delito objeto de la investigación penal no pueda mutar si del resultado del registro se descubren nuevos hechos con apariencia delictiva o incluso que se abra un nuevo procedimiento[11].

10. Martínez Atienza, *Investigación tecnológica en los ciberdelitos*. Ediciones Experiencia, 2020. pág. 13.

11. Sobre todas estas cuestiones es de especial interés la lectura de Fundamento Segundo de la STS 908/2021, de 24 de noviembre (F. J.1º). «*1. El objeto y finalidad del proceso penal determina sin duda alguna la proscripción de la "inquisitio generalis", también llamada "fishing expedition", investigación o causa general.*

Sin duda, el hecho objeto de investigación, con independencia de su complejidad, debe estar delimitado. No es posible iniciar procesos penales para investigar en general a una persona, un entero ámbito *profesional o empresarial o un fenómeno social, por atroces o lamentables que puedan parecer.*

La inquisitio generalis no tiene legitimidad constitucional aun cuando se realice con metas de prevención delictiva. La reacción de la maquinaria del Estado frente a posibles hechos delictivos no debe ser pretexto para una actuación irreflexiva y desproporcionada, pues solo cabe seguir un proceso penal, incluso desde su fase inicial de investigación, cuando existan indicios de la comisión de una infracción penal, sin que quepa su utilización en ausencia de tales indicios.

Como señala la doctrina, un Estado Constitucional repudia la inquisitio generalis o la búsqueda a toda costa de algún tipo de responsabilidad de una persona, ya que genera persecuciones indeterminadas, pesquisas arbitrarias y no sujetas a control jurídico alguno. Existe la proscripción de investigaciones o práctica de pruebas ajenas a lo que es materia de investigación.

En este sentido, el Tribunal Constitucional ha declarado en varias ocasiones (SS 32/1994, de 31 de enero; 63/1996, de 16 de abril; 41/1998, de 24 de febrero y 87/2001, de 2 de abril; 126/2001, de 4 de junio), que un proceso penal instrumentado para la "inquisitio generalis" no es compatible con nuestra Constitución. En la STC 87/2001, de 2 de abril señala que la "inquisición general" es "incompatible,

ISSN: 2951-844X

b) **El principio de idoneidad.**

Escuetamente, pone de relieve la norma procesal que el principio de idoneidad servirá para definir el ámbito objetivo y subjetivo de la medida; la idoneidad será en este caso la utilidad de la medida para la investigación del delito, y sirve de límite para evitar medidas intrusivas que sirvan a fines distintos al de la investigación del delito por el que se siguen diligencias y para evitar que se sacrifiquen derechos fundamentales del investigado y de terceras personas cuando ello no vaya a reportar beneficio alguno a la investigación, así la idoneidad servirá para «determinar la extensión con la que decreta la medida, en lo relativo tanto al sujeto investigado, a los sujetos que pudieren verse afectados y a su duración»[12]. «Una de estas reglas generales es que toda intervención debe ser útil para la comprobación de un delito concreto, por lo que el juez a la hora de autorizar la injerencia debe determinar su ámbito objetivo y subjetivo. La idoneidad significa que la medida ha de acordarse cuando quepa esperar resultados útiles para la investigación (STS 641/2014)»[13].

c) **El principio de excepcionalidad.**

La nota de excepcionalidad conlleva que la medida que se pretenda utilizar no suponga un medio normal y habitual de investigación[14], por lo que la LECrim en su redacción actual exige que se exponga en el auto que autorice la medida la ausencia de otros medios de investigación menos restrictivos para los derechos fundamentales del investigado y que sean igualmente útiles. En la práctica se puede observar que en los oficios policiales en los que se solicitan este tipo de medidas se exponen qué otro tipo de medidas han sido utilizadas (o tratado de ser utilizadas) y el motivo por el que estas ya no pueden ser empleadas y debe recurrirse a estos otros medios más intrusivos.

d) **El principio de necesidad.**

Directamente relacionado con la nota de excepcionalidad, con la que comparte contornos, motivo por la cual la LECrim las regula en el mismo apartado del artículo 588 bis a., la de necesidad supone que el auto que autorice la medida deberá exponer las razones por las cuales «el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito

ciertamente, con los principios que inspiran el proceso penal en un Estado de Derecho como el que consagra la Constitución Española". Sobre este particular también ha tenido ocasión de pronunciarse esta Sala en sentencia núm. 521/2015, de 13 de octubre, en la que con cita y remisión expresa a la sentencia núm. STS 228/2013, de 22 de marzo, señala que "La investigación directa de los hechos con una función que es en parte inquisitiva y en parte acusatoria -dirigida frente a una determinada persona- es la que pueda considerarse integrante de una actividad instructora. Para ello la simple notitia criminis es suficiente para que se ponga en marcha la investigación judicial del delito (SSTC. 169/90, 32/94). La finalidad a que ha de tender toda instrucción criminal es la de averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en la calificación y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos (art. 299 LECrim.)....

...Por tanto, la notitia criminis puede tenerse por un presupuesto o procedibilidad del proceso penal, en la medida en que éste condiciona su inicio a la existencia de un hecho o conjunto de hechos concretos y de fisonomía delictiva, bien entendido que debe tenerse en cuenta que el uso de los poderes inquisitivos que la LECrim, coloca en manos del Instructor puede abocar al descubrimiento de hechos distintos de aquellos que dieron lugar a la incoación del proceso y/o a la implicación de personas distintas de aquellas sobre las que inicialmente recayeron las sospechas. En estos casos aquellos poderes comprenderán también estos otros nuevos hechos, así como las posibles personas implicadas en su comisión».

12. Castillejo Manzanares, «Alguna de las cuestiones que plantean las diligencias de investigación tecnológica», *Revista de derecho y proceso penal*, núm. 45, 2017, pág. 33.
13. STS 634/2019, de 19 de diciembre (F. J. 1.º).
14. STS 156/2012, de 29 de febrero (F. J. 1.º):
«*De la nota de excepcionalidad se deriva que la intervención telefónica no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria. Ciertamente en la mayoría de los supuestos de petición se estará en los umbrales de la investigación judicial —normalmente tal petición será la cabeza de las correspondientes diligencias previas—, pero en todo caso debe acreditarse una previa y suficiente investigación policial que para avanzar necesita, por las dificultades del caso, de la intervención telefónica, por ello la nota de la excepcionalidad, se completa con las de idoneidad y necesidad y subsidiariedad formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional, riesgo sobre el que esta Sala ha llamado la atención varias veces. SSTS 998/2002; 498/2003; 182/2004 y 1130/2009*».

se vea gravemente dificultada sin el recurso a esta medida». No podrán autorizarse, por tanto, medidas de investigación tecnológicas para consolidar el contenido obtenido por material probatorio con el que ya se contaba, sino cuando es el propio avance de la investigación el que está en juego y este no puede producirse sin que se practique la diligencia interesada[15].

e) **El principio de proporcionalidad.**

El principio de proporcionalidad no sirve sino para valorar que «el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros», lo que exige de la autoridad judicial un ejercicio de ponderación en el que deberá valorar todas las circunstancias del caso; el art. 588 bis a.5 LECrim nos indica que para «la valoración del interés público se basará en 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». Nos recuerda el Tribunal Constitucional en su STC 55/1996, de 28 de marzo (F.J.3.º)[16] que la proporcionalidad siempre debe ponerse en relación con la afectación de derechos fundamentales, por lo que no es correcto alegar la vulneración del principio de proporcionalidad de forma autónoma, sino que deberá primero acreditarse qué sacrificio de derechos fundamentales se ha producido para, posteriormente, valorar si en el caso concreto el sacrificio encontraba justificación en el fin perseguido y los medios empleados; así mismo, también nos indica que de forma excepcional también podrá alegarse la vulneración de otros derechos constitucionalmente reconocidos. La principal diferencia, a mi juicio, será el alcance procesal de la vulneración, encontrándonos en el primer lugar en el terreno de la ilicitud probatoria; y en el segundo, en el de la mera irregularidad, con regímenes distintos cuyo análisis se excede de los márgenes en los que se encuentra el presente trabajo.

2. El acceso a dispositivos incautados con ocasión de una diligencia de entrada y registro

La LECrim se preocupa de diferenciar entre aquellos supuestos en que el dispositivo cuyo registro se pretende sea aprehendido durante un registro domiciliario y aquellos en los que la incautación se produzca fuera del domicilio del investigado.

Según la Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, antes de la reforma operada por la LO 13/2015, de 5 de octubre, «el modo habitual de proceder era el de considerar amparado su registro por la resolución judicial que autorizaba la entrada en el domicilio del investigado y el registro de los libros, papeles y demás

15. Sobre el desarrollo de tales principios en la investigación de los delitos de terrorismo, y particularmente, respecto de principio de necesidad puede consultarse Sánchez Gómez, *El derecho de defensa en la investigación de los delitos de terrorismo*, Thomson Reuters Aranzadi, Pamplona, 2017, págs. 231 a 248.

16. Esta apelación genérica al principio de proporcionalidad exige alguna precisión en orden a fijar el objeto exacto y los términos precisos en los que debe desarrollarse el presente proceso constitucional. En primer lugar, debe advertirse que el principio de proporcionalidad no constituye en nuestro ordenamiento constitucional un canon de constitucionalidad autónomo cuya alegación pueda producirse de forma aislada respecto de otros preceptos constitucionales. Es, si quiere decirse así, un principio que cabe inferir de determinados preceptos constitucionales -y en particular de los aquí invocados- y, como tal, opera esencialmente como un criterio de interpretación que permite enjuiciar las posibles vulneraciones de concretas normas constitucionales. Dicho con otras palabras, desde la perspectiva del control de constitucionalidad que nos es propio, no puede invocarse de forma autónoma y aislada el principio de proporcionalidad, ni cabe analizar en abstracto si una actuación de un poder público resulta desproporcionada o no. Si se aduce la existencia de desproporción, debe alegarse primero y enjuiciarse después en qué medida *ésta* afecta al contenido de los preceptos constitucionales invocados: solo cuando la desproporción suponga vulneración de estos preceptos, cabrá declarar la inconstitucionalidad.

El ámbito en el que normalmente y de forma muy particular resulta aplicable el principio de proporcionalidad es el de los derechos fundamentales. Así ha venido reconociéndolo este Tribunal en numerosas sentencias en las que se ha declarado que la desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a un enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que la Constitución garantiza (SSTC 62/82, f. j. 5º); 66/85, f. j. 1º; 19/88, f. j. 8º; 85/92, f. j. 5º; 50/95, f. j. 7º).

(…)

Esta constatación no significa que en algún supuesto concreto no pueda argumentarse a partir del principio de proporcionalidad para concluir en la infracción de otro tipo de preceptos constitucionales. Pero, en todo caso, como queda dicho, siempre deberá indagarse, no la sola existencia de una desproporción entre medios y fines, sino en qué medida esos preceptos resultan vulnerados como consecuencia de la citada desproporción.

ISSN: 2951-844X

documentos del mismo que pudieran tener relación con el delito»; no pudiendo compartir esta afirmación, al menos rechazando que esta fuese la línea jurisprudencial dominante, pues la LO 13/2015, de 5 de octubre, no hace sino positivizar los requisitos que había establecido la jurisprudencia con anterioridad, siendo así que ya en la propia STS 342/2013, citada anteriormente y citada en la propia Circular, se indicaba expresamente que la autorización judicial para la entrada en el domicilio del investigado no habilitaba para el registro de los dispositivos allí hallados[17].

De cualquier modo, la reforma de 2015 prevé la obligatoriedad de una motivación individualizada para poder acordar esta medida sin que la norma haga referencia alguna a si debe formar un apartado distinto dentro de la propia autorización de la entrada domiciliaria o si debe ser una resolución distinta.

A nuestro modo de ver, aunque razones de eficiencia procesal aconsejan introducir esta autorización y motivación dentro de un apartado contenido en el mismo auto que autorice el registro domiciliario, una resolución autónoma garantiza que todos los argumentos empleados sean genuinos y evita el trasvase de argumentos y la motivación por remisión a motivos anteriores expuestos para autorizar la entrada en el domicilio.

En casos en que no se haya autorizado expresamente el registro de dispositivos y durante la entrada en el domicilio estos aparezcan, podrán ser incautados, si bien, para poder proceder a su registro, este deberá posteriormente ser autorizado por el juez competente (art. 588 sexies a.2 de la LECrim). Todo ello sin perjuicio de los supuestos de urgencia y de consentimiento del investigado.

3. El acceso a dispositivos incautados fuera del domicilio

El art. 588 sexies b) de la LECrim extiende la obligación de recabar autorización judicial a aquellos casos en los que se pretenda acceder a dispositivos incautados con independencia de un registro domiciliario, aunque con una dinámica distinta.

En este caso, la LECrim prevé que la autorización para el registro sea posterior a la incautación del dispositivo; en el caso anterior, se podía autorizar el registro de aquello que aún estaba por individualizar siempre que estuviera dentro del ámbito objetivo y subjetivo de la medida autorizada por el Juez.

Este régimen en el que primero se descubre qué dispositivos existen y posteriormente se autoriza el registro de cuantos se consideren de interés, podía perfectamente haber sido el previsto para los supuestos de registro con ocasión de entrada domiciliaria; no se termina de entender del todo el motivo de crear esta dualidad cuando además esta sería más garantista con el derecho del investigado a la exclusión de su entorno virtual, pues la labor previa de identificación de los dispositivos encontrados permitirá que se excluya del registro aquellos cuyo análisis se pueda prever inidóneo para clarificar los hechos o innecesario para proseguir la investigación.

Sobre el proceder marcado por la norma, el criterio de la FGE, según su Circular 5/2019, de 6 de marzo, es que, aunque «la previsión literal del precepto alcanzaría únicamente a los casos en los que se haya producido la previa aprehensión del dispositivo, solicitándose posteriormente autorización judicial para su registro, no existe inconveniente en interpretar que también resultará aplicable cuando la resolución judicial preceda a la incautación». No puede compartirse esta interpretación de una norma cuya literalidad marca una temporalidad muy clara y no hace sino garantizar una correcta labor fijación de los términos, alcance y garantía de los registros, en unos supuestos en los que durante el momento de la incautación la norma guarda silencio sobre la presencia del fedatario público judicial.

Esto último será especialmente interesante en los casos de incautación de equipos tecnológicos que no almacenan datos en su interior, sino que trabajan con datos almacenados en la nube, pudiendo ser los archivos eliminados remotamente en caso de demora en su acceso, incidiendo Portal Manrubia[18] en que el uso por parte de los investi-

17. Según la ponencia de la Sala: *«(…) tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización 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 utilización de las nuevas tecnologías (…). La necesidad de que toda resolución judicial llamada a legitimar un acto de injerencia en los derechos fundamentales del investigado sea interpretada conforme a su estricta literalidad, forma parte de las notas definitorias de nuestro sistema constitucional. En esta materia no caben las interpretaciones extensivas ni la elasticidad como fuente inspiradora a la hora de delimitar los exactos términos de la autorización concedida*.

18. Portal Manrubia, «La incorporación de los dispositivos de almacenamiento masivo en el procedimiento penal», *Revista Aranzadi Doctrinal*, núm. 2, 2019, p. 17.

gados de estos sistemas de *cloud computing* «puede comportar dificultades para la investigación. A este respecto, el aparato informático objeto de la incautación puede procesar con un software remoto no instalado, amén de la gran cantidad de datos digitales que pueden ser almacenados y obtenidos, velozmente, a partir de una mínima interacción con el proveedor. La adquisición de los datos digitales se efectúa de modo dinámico mediante la conexión a internet, pudiendo ser modificados y borrados con facilidad, sobre todo si se quiere compartir la información con otros usuarios».

En estos casos, una autorización previa que permita el acceso al dispositivo en la nube «siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este», servirá de gran ayuda a los investigadores. En caso contrario, los investigadores podrán valerse de la facultad que les otorga el art. 588 octies de la LECrim hasta conseguir recabar una ampliación de la autorización[19].

4. Términos y alcance del registro

El art. 588 sexies c) de la LECrim impone al juez la obligación de fijar los términos y alcance del registro, así como fijar las condiciones necesarias para asegurar la integridad de los datos y garantizar la eventual práctica de un informe pericial.

Conforme el apartado segundo del precepto indicado, la regla general será que no se proceda a la incautación de los dispositivos siempre que pueda realizarse una copia de su contenido en condiciones que aseguren la autenticidad e integridad de los datos y la incautación pudiera causar grave perjuicio a su titular, a menos que estos dispositivos constituyan el objeto o instrumento del delito. Es decir, la regla general es que se trabaje sobre copias en lugar de sobre el propio dispositivo, lo que, además, es la opción más aconsejable a efectos de poder garantizar la exactitud de los datos analizados.

La LECrim guarda silencio sobre la forma en que deberá llevarse a cabo la medida, renunciando incluso a establecer pautas generales, por lo que la forma en que se desarrolle la medida y el sistema de garantías debe ser establecido por el juez de instrucción, no faltando en la doctrina y la jurisprudencia proposiciones sobre formas correctas de practicar la diligencia.

Según Fernández-Gallardo[20], la obligación de concretar los términos y alcance del registro conlleva que el auto autorizante «habrá de concretar, entre otros extremos, si se autoriza la realización de un clonado o volcado, que consiste en la realización de una «copia espejo» o bit a bit de la información original, o bien la realización de una copia lógica, es decir, una copia selectiva de ciertas carpetas o ficheros», indicando que será aconsejable su clasificación por titularidad y clase de dato, lo que no parece tarea fácil si no se cuenta con la colaboración del sujeto pasivo de la medida y los dispositivos son de uso compartido.

En la práctica no es extraño el uso de softwares como *Autopsy* y similares que sirven para rastrear la ubicación de la información de interés dentro del contenido de una memoria, sirviendo a los agentes encargados del registro tanto para poder hallar la información concreta necesitada de forma rápida como para minimizar la intensidad del sacrificio de la privacidad e intimidad del investigado; esto servirá tanto para realizar las copias lógicas como para analizar mejor el contenido de los volcados.

Asimismo, sobre el aseguramiento de la integridad de los datos, debe tenerse en consideración que no serán las mismas garantías en caso de clonado que en caso de copia lógica. Es aconsejable realizar dos copias, una para su análisis y otra para su custodia por el letrado de la Administración de Justicia, siendo indiferente el tipo de copia ante el que nos encontremos.

De la integridad de los datos en caso de volcado, el AAP de Badajoz 271/2020, de 5 de octubre, ECLI:ES:APBA:2020:331A (F.J.2.º), sostiene que «La conservación de la cadena de custodia de una prueba informática es posible mediante el código "hash" de cada una de las evidencias intervenidas, en el mismo momento en el que le son incautadas al investigado o, si esto no es posible, que las pruebas sean precintadas, etiquetadas, inventariadas y almacenadas para su posterior volcado y el cálculo de su código "hash" ante funcionario policial o letrado de la Administración de Justicia. Además, el cálculo del código "hash" deberá producirse evitando en todo momento que éste se conecte a la red, aislándolo para ello con una " jaula de Faraday"».

19. Prevé el citado precepto que «[e]l Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes».

20. Fernández-Gallardo, «Registro de dispositivos de almacenamiento masivo de información», *Dereito revista xurídica da Universidade de Santiago de Compostela*, vol. 25, núm. 2, 2016, pp. 15-17.

ISSN: 2951-844X

El *hash* es un código con una longitud de 40 caracteres de muy diverso tipo, generado mediante algoritmos, con los que se identifican grupos de datos, modificándose este código en caso de haber alguna modificación en los mismos[21]. Advierte Fernández-Gallardo[22] que el mero hecho de conectar la memoria con la copia a un ordenador ya puede alterar el *hash*, por lo que deberán utilizarse en el análisis de los datos equipos que bloqueen la posibilidad de escritura para, así, asegurar la coincidencia entre el original y la copia analizada. A pesar de todo, pueden observarse sentencias en las cuales la no coincidencia del código hash no determina necesariamente la invalidez de la prueba[23].

En caso de copias lógicas, en las que se procede primero a un análisis preliminar del contenido del dispositivo para una posterior selección de los archivos de interés, que son los únicos que serán copiados, también es posible garantizar su autenticidad mediante el *hash*; los problemas, en caso de haberlos, llegarán por otra vía.

En el caso de volcado de datos se parte de un todo en el que habrá tanto elementos de cargo como de descargo, en el caso de la copia lógica se parte de un proceso de selección en el que únicamente se garantizará la autenticidad e integridad de una serie de datos concretos. Quienes participen en el proceso de selección de datos deberán ser muy escrupulosos con el cumplimiento de la obligación de indagar tanto sobre las circunstancias adversas como sobre las favorables al investigado, derivadas del art. 2 LECrim[24], pues en caso de que la selección únicamente se preocupe de recabar material de cargo, el material de descargo no gozará de la garantía de autenticidad de que sí tendrá el que habrá de sustentar una eventual acusación. Por ello, varios autores y la FGE en su Circular 5/2019[25] han venido haciendo hincapié en lo altamente recomendable que se revela aquí la presencia del letrado de la Administración de Justicia durante el proceso de selección de los archivos y carpetas a copiar, añadiendo Fernández Rodríguez[26] que, en el caso de copias lógicas, se convierte en necesaria la presencia del investigado. En idéntico sentido, la Circular 5/2019 FGE señala que «cuando se lleve a cabo una copia selectiva de archivos deberá requerirse siempre su presencia, pues no se tratará de una simple diligencia de copia de archivos, sino que, en el propio acto, habrá que decidir también acerca de la selección de esos archivos, lo que requiere contradicción para garantizar el derecho de defensa del afectado». Según Sánchez Gómez[27], «[e]l contradictorio sobre la prueba concurre cuando se ha garantizado que las partes han podido hacer las observaciones pertinentes y adecuadas a su derecho», aunque en la práctica poco lugar habrá para la contradicción cuando la selección de archivos se realice directamente por la Policía Judicial. Esta problemática aparejada a las copias lógicas, cuya solución no es sencilla sin cambios legislativos, a la que debe añadírsele la línea del TS en relación a la imposibilidad de presumir la existencia de vulneraciones de derechos fundamentales cuando se desconocen las circunstancias en las que se desarrollan las diligencias[28],

21. SAN 9/2022, de 31 de marzo (F.J.3.º), afirma que la «firma hash es el resultado de la aplicación de un algoritmo matemático que se supone irreversible. Se hace esta firma para decir que un dispositivo o que un fichero tiene una huella dactilar, algo que es único para este dispositivo en el momento de realizarlo y, en el supuesto caso de intentar alterar este dispositivo, se puede comprobar con esta huella digital que ha sido alterado este fichero, dispositivo o imagen al que se haya aplicado el hash».
22. Fernández-Gallardo, «Registro de dispositivos de almacenamiento masivo de información», *Dereito revista xurídica da Universidade de Santiago de Compostela*, vol. 25, núm. 2, 2016, *ob. cit.*, pág. 17.
23. Por ejemplo, la SAP Madrid 323/2020, de 9 de julio.
24. La STC 136/1992, de 13 de octubre, señala que «es preciso recordar, por lo que se refiere a esta concreta cuestión, de una parte, que la instrucción supone una investigación objetiva de la verdad, en la que el instructor ha de indagar, consignar y apreciar las circunstancias, tanto adversas como favorables al imputado (art. 2 LECr.), y de otra, que para garantizar la independencia judicial surge en la esfera del proceso la abstención y recusación, con el fin de evitar la privación en los órganos jurisdiccionales de la idoneidad subjetiva o de las condiciones de imparcialidad o de neutralidad (SSTC 47/1982 y 44/1985, entre otras muchas)».
25. Expone la Circular que «la mejor forma de garantizar qué se copia, cómo se copia y la integridad de la copia, será su realización a presencia y bajo la fe del letrado de la Administración de Justicia».
26. Fernández Rodríguez, «Algunas consideraciones a partir de la regulación del registro de dispositivos de almacenamiento masivo de la información», *Diario La Ley*, núm. 9433, Sección Tribuna, de 11 de junio de 2019.
«Aunque la presencia del interesado no sea necesaria para llevar a cabo el copiado de los datos, si la práctica se realiza durante una diligencia de entrada y registro sería lógica la permisión para presenciar el copiado y se convertiría en necesaria cuando se haga una copia selectiva de los archivos».
27. Sánchez Gómez, *El derecho de defensa en la investigación de los delitos de terrorismo*, ob. cit., pág. 245.
28. Por todas, STS 201/2022, de 3 de marzo de 2022 (F.J.5º):
«*Esta Sala Segunda, en sentencias 362/2011, de 6-5, 628/2010, de 1-7, 406/2010, de 11-5, 6/2010, de 27-1, que la premisa de la que se quiere partir -implícita pero evidente- que no puede admitirse es que, en principio, hay que presumir que las actuaciones judiciales y policiales son ilegitimas e irregulares, vulneradoras de derechos fundamentales, mientras no conste lo contrario.*
Ello supondría la paradoja de que mientras que tratándose de los acusados ha de presumirse su inocencia, en tanto no se prueba su culpabilidad (art. 29.2 CE), a los Jueces y Tribunales, en el mismo marco procesal, ha de resumírseles una actuación contraria a la Constitución a las Leyes en tanto no se prueba que han actuado conforme a Derecho. Frente a tal premisa, hemos de afirmar que en el derecho

lleva a desaconsejar la práctica de este tipo de copias si no se quiere colocar al investigado en situación de indefensión, pues el legislador ha decidido voluntariamente encomendarse al acierto del juez en la determinación de los términos del registro y la fijación de garantías.

No existe un solo tipo de autorización judicial para el registro de dispositivos de almacenamiento masivo de información y cada tipo tiene unas exigencias específicas que determinará una mayor o menor exhaustividad en la fijación del término y alcance del registro. Se pueden resumir los tipos de autorización en: a) autorización previa incautación, b) autorización posterior a la incautación, c) ampliación de una autorización anterior y d) convalidación de un registro de urgencia.

a) **Autorización previa incautación.**

En estos casos, el auto que se dicte deberá prever los tipos de dispositivos que puedan ser hallados y la posibilidad de que algunos de los dispositivos que se intervengan puedan actuar conectados a la nube, a bases de datos o en sistemas de mensajería online. Este tipo de resoluciones deberán ser muy exhaustivas y englobar gran cantidad de supuestos, pues recuérdese que la ya varias veces citada STS 342/2013 incidía en la exigencia de que «toda resolución judicial llamada a legitimar un acto de injerencia en los derechos fundamentales del investigado sea interpretada conforme a su estricta literalidad, forma parte de las notas definitorias de nuestro sistema constitucional. En esta materia no caben las interpretaciones extensivas ni la elasticidad como fuente inspiradora a la hora de delimitar los exactos términos de la autorización concedida». En virtud de lo anterior, no será posible extender el registro a dispositivos o sistemas informáticos cuya existencia no haya sido prevista en la autorización judicial. La resolución, a fin de evitar el excesivo sacrificio de los derechos fundamentales del investigado, deberá especificar que únicamente podrá extenderse a los dispositivos que previsiblemente puedan estar relacionados con la perpetración del hecho delictivo o a aquellos en los que se puedan pruebas de su comisión.

b) **Autorización posterior a la incautación.**

En estos casos, una vez que al juez le llega la solicitud de registro, este ya conoce qué bienes concretos han sido hallados y estos han sido debidamente individualizados y clasificados; no conoce su contenido, pero sí conoce sus características técnicas, el lugar concreto en el que fueron hallados, etc., lo que le permitirá evaluar *ex ante* qué tipo de datos podrá obtener de cada uno de los dispositivos. Según el artículo 588 sexies.b de la LECrim, una vez se haya dado cuenta al juez de los efectos incautados, si «éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización». El hecho de que el legislador haya impuesto al juez la labor de valorar qué posible contenido puede albergar los dispositivos y solamente autorizar los registros indispensables supone una garantía más para el investigado, pues de este modo se ayuda a minimizar la intensidad de la injerencia.

c) **Ampliación de una autorización anterior.**

La prohibición de extender los límites de la autorización ha llevado a que el legislador se ocupe de aquellos casos en los que la autorización judicial no cubre el registro de alguno de los dispositivos que puedan llegar a incautarse o de otros sistemas en los que se sospeche que puedan encontrarse alojados los datos de interés (arts. 588 sexies.a.2 y 588 sexies.b.3 de la LECrim). En los supuestos de necesidad de ampliación, surgirá habitualmente el problema de tener que determinar si nos encontramos ante supuestos de urgente necesidad que requieren una actuación inmediata o si puede esperarse a recabar la ampliación de la autorización. La potestad que otorga el art. 588 octies de la LECrim tanto al Ministerio Fiscal como a la Policía Judicial para que puedan ordenar la conservación de datos alojados en sistemas informáticos de almacenamiento, unida a la de poder permanecer los

a la presunción de inocencia ni el principio "in dubio pro reo", que siempre deben proteger a los acusados, pueden llegar a significar que salvo que se acredite lo contrario, las actuaciones de las Autoridades son, en principio, ilícitas e ilegitimas. El principio de presunción de inocencia no puede extender su eficacia hasta esos absurdos extremos.

En efecto la nulidad de los actos procesales sólo puede basarse en algunas de las causas estrictamente reguladas en el art. 238 LOPJ con la consecuencia de la perdida de efectos que tratándose de la vulneración de derechos fundamentales, impone el art. 11 de la misma ley. Sin embargo, declarar la nulidad de unas escuchas porque la legitimidad de la obtención del número telefónico no puede presumirse, supone crear una categoría inédita en nuestro sistema procesal. Estaríamos ante la creación jurisprudencial de la creación jurisprudencial de la nulidad presunta, aquélla predicable de actos limitativos de derechos, aparentemente válidos, pero a los que privamos de efectos al no constar la legitimidad de otro acto precedente».

ISSN: 2951-844X

dispositivos incautados hasta recabar la debida autorización, minimiza el riesgo de perder información durante el tiempo que transcurra entre la solicitud de ampliación y la respuesta por parte del juzgado, por lo que entiendo que la urgente necesidad deberá venir marcada por las circunstancias concretas del caso y no por las características de los dispositivos.

d) **Convalidación de un registro de urgencia.**

La norma distingue dos supuestos distintos en los cuales se podrá proceder al registro de urgencia sometido a posterior convalidación judicial. Ni los tribunales ni la doctrina han tratado de definir qué debe entenderse por urgente a estos efectos, quizá tampoco sea conveniente crear definiciones que encorseten aquello que debe adaptarse al caso concreto; lo que sí ha venido indicando de forma reiterada el TC es que la valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante*, y es susceptible de control judicial *ex post*. Además, la constatación *ex post* de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales.

En el apartado tercero del artículo 588 sexies c) de la LECrim se prevé la posibilidad de acceder de urgencia, durante la ejecución de un registro de dispositivos, a los sistemas informáticos en los que se puedan encontrar alojados los datos de interés para la investigación a los que se pueda acceder «por medio del sistema inicial o estén disponibles para este». El punto de partida es una resolución judicial previa que, por no prever que el dispositivo registrado pudiera estar conectado a otro sistema informático, necesitaba ser ampliada; es decir, existe un defecto en la fijación del término y alcance del registro. En este caso, la ampliación podrá ser autorizada por la Policía Judicial o por el fiscal, y se deberá dar cuenta al juez de forma inmediata, con un límite máximo de 24 horas, debiendo el juez revocar o confirmar la actuación en las 72 horas siguientes a ordenarse la interceptación.

En el caso del apartado cuarto del mismo artículo el supuesto de hecho es distinto, no ha habido fijación alguna y la deberá realizar la propia Policía Judicial. Se trata ahora de dar validez a la entrada en el proceso ve la información obtenida en un registro de los dispositivos sin solución de continuidad con su incautación. Existirán situaciones en las que, para la prosecución de un «fin constitucionalmente legítimo»[29], será absolutamente imprescindible acceder a los dispositivos del sujeto pasivo de la medida en el mismo momento en que se le detiene. Pueden imaginarse muchos escenarios en los que la respuesta inmediata de las autoridades conseguirá salvar la vida de otras personas o proteger otros muchos derechos e intereses de terceros que, tras la debida ponderación, deben primar sobre el derecho de exclusión del entorno virtual del investigado. Será la Policía Judicial la que realice el examen directo del dispositivo, dando cuenta al juez de forma inmediata, con un límite máximo de 24 horas, debiendo el juez revocar o confirmar la actuación en las 72 horas siguientes a ordenarse la medida.

Será la autoridad policial (también podrá ser el fiscal en el caso del art. 588 sexies c) 3 de la LECrim) la que deba analizar si se dan todos los presupuestos para acordar el registro de los dispositivos y equipos, además del requisito de urgente necesidad, motivándolo en el oficio que se remita al juzgado. Algunos autores como Arrabal Platero[30] vienen denunciando el peligro que supone esta habilitación para casos de urgente necesidad, pues aunque

29. La Circular 5/2009, de 6 de marzo, de la Fiscalía General del Estado refiere que *«el interés constitucionalmente legítimo enlaza, como señala la Circular 1/2013, con el art. 8.2 del CEDH que, para la admisibilidad de la injerencia de la autoridad pública en el derecho a la vida privada, considera necesario que la medida persiga a alguna de las siguientes finalidades: la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás. De entre ellas, señala la lucha contra el delito como la que dará normalmente cobertura a la actuación policial. La STC n.º 207/1996, de 16 de diciembre, considera como intereses constitucionalmente legítimos para la limitación de derechos fundamentales, la actuación del ius puniendi del Estado, la investigación de los delitos y la determinación de hechos relevantes para el proceso penal y, la STS n.º 133/2016, de 24 de febrero, con cita de la STC n.º 115/2013, establece:* «la *actuación de los policías en el marco de la investigación de un delito y el descubrimiento de los delincuentes,* «constituye *un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana, bienes igualmente reconocidos en los artículos 10.1 y 104.1*».

30. Véase Arrabal Platero, «La incorporación al proceso de las evidencias obtenidas de equipos informáticos y de dispositivos de almacenamiento masivo de información. El expurgo del contenido irrelevante», *Revista Aranzadi de derecho y nuevas tecnologías.* N.º. 56, 2021 cuando refiere que «*esta legitimación (inicial o de ampliación de la medida) sin previo control del juez reduce notablemente la garantía constitucional del examen de su proporcionalidad, motivo por el cual ha sido muy criticada por la doctrina. Y ello porque puede darse la situación en la que los agentes accedan a los datos de un ordenador sobre la base de motivos de urgencia que posteriormente no sean convalidados judicialmente. Esta información, aunque no puedan configurarse como material probatorio, puede servir para avanzar en la investigación de una manera fraudulenta*».

no se produzca la posterior convalidación, ya se habrá avanzado en la investigación de forma fraudulenta. No puede compartirse esta afirmación a la luz de la jurisprudencia que delimita los efectos procesales entre la ilicitud y la irregularidad probatoria[31]. En el supuesto de que la prueba sea inválida, se considerará que esa información que se obtiene queda vetada para ser hallada por otros medios distintos. Esto no hace sino garantizar que, en el caso de que la urgente necesidad se utilice de forma fraudulenta, está vulneración de derechos fundamentales no podrá tener efectos procesales perjudiciales para el investigado.

5. El consentimiento del investigado

Supone la excepción a la obligación de contar con resolución judicial habilitante. La LECrim nada dice respecto a la validez de un posible consentimiento del investigado para la práctica de la diligencia, si bien esta era una posibilidad que la doctrina del Tribunal Constitucional venía admitiendo, por ejemplo, en la ya citada STC 173/2011, por lo que debe entenderse que el hecho de que la nueva regulación guarde silencio al respecto no implica que no puedan realizarse registro de dispositivos únicamente amparados en el consentimiento del investigado.

Únicamente surtirá efectos el consentimiento válido. Lo analiza Sánchez Gómez[32] conectando esta cuestión con el consentimiento para el registro domiciliario, expresamente previsto en el artículo 18.2 de la CE y destacando los siguientes requisitos para su validez:

a) Deberá ser prestado por mayor de edad sin restricciones a su capacidad de obrar.
b) Solamente será válido el consentimiento consciente y libre, «lo cual requiere: i) que no esté invalidado por error, violencia o intimidación de cualquier clase; ii) que no se condicione a circunstancia alguna periférica, como promesas de cualquier actuación policial, del signo que sean; iii) que si el que va a conceder el consentimiento se encuentra detenido, no puede válidamente prestar tal consentimiento si no es con asistencia de Letrado, lo que así se hará constar por diligencia policial».
c) No se requiere que el consentimiento sea expreso, pero «[e]l consentimiento tácito ha de constar de modo inequívoco mediante actos propios tanto de no oposición como, y sobre todo, de colaboración, pues la duda sobre el consentimiento presunto hay que resolverla en favor de la no autorización, en virtud del principio *in dubio libertas* y el criterio declarado por el Tribunal Constitucional de interpretar siempre las normas en el sentido más favorable a los derechos fundamentales de la persona».
d) Ya haya sido otorgado de forma oral o escrita, debe estar documentado.
e) Si el dispositivo puede ser utilizado por más de un usuario, «debe prevalecer tanto los criterios jurisprudenciales de contraposición de intereses, como la imposibilidad de intervención ante la expresa negativa de algún usuario si no existiesen cuentas de acceso diferenciadas», con mayores dificultades si solamente existe una cuenta en el terminal.
f) No puede entenderse el consentimiento extendido a fines distintos del cual fue prestado.

31. Por todas, la STS 201/2022, de 3 de marzo (F.J.7.º) indica lo siguiente:
«*Por último, la interpretación que del art. 11.1 LOPJ ha hecho tanto el TC como esta Sala, permite sostener en nuestro ordenamiento un concepto de prueba ilícita referido exclusivamente a la que es obtenida violentando derechos y libertades fundamentales, de manera que por definición se concibe otra suerte de ilicitud probatoria, simplemente ordinaria, que se ha dado en llamar prueba irregular, cuyos efectos no podrían ser parejos a la anterior por mor del derecho fundamental a la prueba (art. 24.2 CE) (STS 6/2010, de 27-1).*
Las diferencias entre la prueba ilícita y la prueba irregular, en orden a la eficacia probatoria en el proceso penal, no son sin embargo apreciables en un primer grado, ya que tanto una como otra carecen de virtualidad al respecto, dependiendo en el segundo caso de la naturaleza, gravedad y acumulación de irregularidades y sobre todo de la indefensión provocada (art. 238.1 LOPJ).
La diferencia entre la prueba ilícita y la prueba irregular, por tanto, habrá de advertirse en un segundo grado, en relación con las pruebas relacionadas con ellas, ya que las derivadas de las pruebas ilícitas se impone asimismo la ineficacia como lógica consecuencia de una fuente de contaminación la llamada en el ámbito *anglosajón doctrina del fruto podrido o manchado ("the tainted fruti") o genéricamente, doctrina de los "frutos del* árbol *envenenado (the fruti o the poisonons tree doctrine") mientras que para las derivadas de las simplemente irregulares no se produce tal radical consecuencia, por lo dispuesto en el art. 242 LOPJ, y nada obsta a que la convicción se obtenga por otros acreditamientos en la materia.*
Esta diferencia se resuelve en la práctica, por tanto, en la posibilidad de recuperación del material probatorio evidenciado por la prueba irregular, mediante su conversión en algún otro tipo de prueba subsidiaria, generalmente la testifical o la confesión, a modo de subsanación, posibilidad que es impensable en el caso de prueba ilícita».

32. Sánchez Gómez, *El tratamiento integral de la entrada y el registro en el marco del proceso penal*, Wolters Kluwer, Madrid, 2021, págs. 168 y ss.

ISSN: 2951-844X

Un buen ejemplo práctico sobre la aplicación de los requisitos anteriormente expuestos lo encontramos en la SAP Madrid 353/2020, de 24 de septiembre (F.J.2.º), en la que se absuelve a quien había sido condenado en primera instancia por un delito contra la propiedad intelectual, al entender que se había vulnerado su derecho de exclusión del entorno digital por ausencia de consentimiento válido por las circunstancias del ambiente en el que el mismo se prestó:

> «(…) no puede llegar esta Sala a la conclusión de que el acusado consintiese que la Policía Municipal se llevasen los discos duros del ordenador y mucho menos que se accediese al contenido del mismo, como tampoco que ofreciese un consentimiento valido al acceso a los propios ordenadores para extraer la información sobre los sistemas operativos de los mismos y ello por cuanto, no consta en la causa ningún consentimiento expreso del acusado y tampoco se desprende de las declaraciones prestadas, tanto por el acusado como por los policías municipales, que consintiese tácitamente el mismo, pues lo que ha asegurado el acusado y también los Policías, es que los citados agentes policiales acudieron al locutorio propiedad del acusado y le informaron de que se iba a realizar una inspección rutinaria del mismo, no diciendo nada al respecto el acusado, si bien en el trascurso de dicha inspección rutinaria, por los policías actuantes se accedió a los ordenadores, tras decirle al acusado que desbloquease las pantallas, que se hallaban bloqueadas, para poder acceder a los mismos, haciéndolo así el acusado, y tras el examen policial de los ordenadores para extraer la información sobre el sistema operativo de los mismos, le dijeron que se llevaban los discos duros y se los llevaron.
>
> (…) no puede entenderse, del modo que se produjo la inspección del locutorio, que el consentimiento del acusado se realizase de manera tácita de forma inequívoca y libre, al no serle preguntado por dichos agentes policiales sobre si consentía el acceso a los ordenadores, ni informado de la investigación que estaban llevando a cabo sobre la posible comisión de un delito, en este caso, contra la propiedad intelectual por parte del mismo, limitándose el acusado a obedecer los mandatos policiales, encontrándose en el interior del local tres policías municipales, que indudablemente configura un entorno ambiental que aminora la serenidad del acusado. Sin que la falta de oposición signifique en todos los casos consentimiento tácito. (STS de 287/19 de abril de 2017). Y no consta que prestase verbalmente el mismo en el atestado policial, debiéndose resolver en cualquier caso la duda (que no se ha generado en este caso) en favor de la no autorización».

III. LOS INTERVINIENTES EN LA MEDIDA

Tan importante como que la medida sea autorizada o convalidada judicialmente atendiendo a los principios enumerados en la norma y enunciados desde antiguo por el TC es que en el diseño de la ejecución de la medida se seleccionen a los actores correctos y se les asigne el mejor papel posible dentro del marco de medidas para asegurar las garantías del procesado y la integridad de los datos.

Así, resumidamente, la autorización judicial deberá designar a los agentes de las unidades de Policía Judicial que han de ejecutar la incautación y registro, establecer en qué momentos deberá intervenir el fedatario público judicial, otorgar al investigado la posibilidad de contradicción en casos de realización de copias selectivas y dar la oportunidad a su defensa letrada de asesorarle acerca de las consecuencias de un eventual consentimiento. Por último, con relación a las personas que intervienen, no puede olvidarse que cualquier persona distinta del investigado y las personas dispensadas de declarar contra este están obligadas a atender los requerimientos de la autoridad para colaborar en el acceso a los dispositivos y sistemas de almacenamiento de datos.

1. Policía Judicial

Los artículos 588 bis b) 2.5.º y 588 bis c) 3 d) de la LECrim exigen que tanto la resolución judicial que autorice la medida como la solicitud previa del Ministerio Fiscal o la Policía Judicial indiquen cuál ha de ser la «unidad investigadora de la Policía Judicial» que se hará cargo de la intervención. Para poder completar, este concepto deberá acudirse a los artículos 29 y siguientes de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (LOFCS) y a Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial (RDPJ). Las unidades de Policía Judicial se formarán atendiendo a criterios territoriales y de especialización delictual, pudiendo quedar total o parcialmente adscritas a determinados juzgados, tribunales o al Ministerio Fiscal (art. 30 de la LOFCS), dependiendo orgánicamente del Ministerio del Interior y funcionalmente de los juzgados, tribunales o Fiscalía que conozca del asunto objeto de su investigación (art. 31 de la LOFCS). Las unidades se formarán, como regla general, con la provincia como base territorial, si bien podrán crearse unidades de ámbito superior a la provincia por razones de especialización delictual o de técnicas de investigación (art. 9 del RDPJ). Esta que se ha descrito es la que viene

denominándose como Policía Judicial en sentido estricto, si bien existirán otros cuerpos que entrarán dentro del concepto más amplio de Policía Judicial[33] que actuarán dentro de su propio ámbito.

La designación de la unidad que habrá de realizar la diligencia, que se encuentra dentro de las disposiciones comunes a las medidas de investigación tecnológica, entiendo que no debería ser de aplicación al registro de dispositivos de almacenamiento masivo de datos por innecesaria y ser susceptible de causar problemas a la investigación. En el registro de dispositivos físicos de almacenamiento de datos, al contrario que ocurre con las demás medidas de investigación tecnológica, siempre han actuar varias unidades. Esto es un condicionante impuesto por su condición de medida plurifásica en la que actuarán unidades con muy distinta especialización; piénsese en todos los posibles intervinientes en caso de realizarse entrada domiciliaria, registro domiciliario, realización directa de copias y análisis de datos (que, presumiblemente, requerirá de apoyo de otras unidades con mayor especialización de ámbito superior al provincial en caso de imposibilidad de acceder a los datos si estos se encuentran protegidos).

Respecto a su carácter de innecesario, ninguna duda cabe de que en el resto de investigaciones tecnológicas es imprescindible que quede determinado desde un inicio quienes tendrán acceso a la información, pues la misma se obtiene subrepticiamente, pero este no es el caso del registro físico de dispositivos de almacenamiento de datos en el que el investigado, desde el inicio, sabe que los equipos han sido incautados o se han realizado copias de los mismos en su presencia durante el registro domiciliario. Sobre su carácter de medida de control también se ha pronunciado la FGE en su Circular 1/2019, de 6 de marzo[34]. De igual modo, tampoco tiene mucho sentido que sea de aplicación el art. 588 bis d) de la LECrim, que impone el carácter de secreto de la medida, pues el investigado ya conoce la existencia de la instrucción judicial tras haberse producido una entrada en su domicilio o tras habérsele incautado sus bienes durante otra diligencia, así como es perfectamente conocedor del contenido existente en el interior de los dispositivos[35].

Sobre los problemas asociados, estos pueden provenir de: a) casos en los que en el auto no se autoriza a todas las unidades que intervienen; b) otro supuesto —habitual en la práctica— es que quien solicita la medida, por no pertenecer a la unidad que ha de analizar los datos, acaba teniendo que pedir un cambio de designación de unidad especializada, porque esta no puede hacer frente al encargo por ser de una complejidad tal que requiere de una unidad con mayor especialización[36] o por sobrecarga de trabajo. En el primer caso podría arrastrarse a la diligencia hacia su invalidez, por ser jurisprudencia consolidada aquella que ya ha sido expuesta relativa a la imposibilidad de extender los límites de una resolución judicial; a efectos prácticos, el criterio que seguirá el Ministerio Fiscal, según la Circular 1/2019 de la FGE, es que «[l]a omisión de este requisito, su deficiencia o error no debería tener trascendencia constitucional que invalidara la resolución, salvo que ese déficit de control judicial resultara incrementado por otras circunstancias». En el segundo, la solicitud del cambio de unidad llevará a demoras innecesarias en la práctica de una diligencia que en la gran mayoría de casos requerirá de la mayor agilidad en la obtención de resultados para poder continuar con la investigación.

Sobre la intervención de la Policía Judicial, apunta Castillejo Manzanares[37] hacia «la posibilidad de que esta medida se conceda asociada a la del agente encubierto informático que se ha regulado *ex novo* en el apartado 6.º del art. 282 bis LECrim», siendo este un agente de Policía Judicial que actúa en canales cerrados de comunicación «a modo de observador participante»[38] que podrá intercambiar archivos ilícitos y analizar los resultados de los algo-

33. Acuerdo de Pleno no Jurisdiccional de la Sala II de 14 de noviembre de 2003.
«PRIMERO: "el artículo 283 de la l.e. criminal no se encuentra derogado, si bien debe ser actualizado en su interpretación.
SEGUNDO: el servicio de vigilancia aduanera no constituye policía judicial en sentido estricto, pero sí en sentido genérico del art. 283.1 de la lecriminal, que sigue vigente conforme establece la disposición adicional primera de la lo 12/95, de 12 de diciembre sobre represión del contrabando. En el ámbito de los delitos contemplados en el mismo tiene encomendadas funciones propias de policía judicial, que debe ejercer en coordinación con otros cuerpos policiales y bajo la dependencia de los jueces de instrucción y del ministerio fiscal.
TERCERO: las actuaciones realizadas por el servicio de vigilancia aduanera en el referido ámbito de competencia son procesalmente válidas"».

34. «La identificación de la unidad policial no venía siendo exigida por la jurisprudencia (en este sentido, STS n.º 1563/2005, de 24 de enero), constituyendo ahora una novedad. Su inclusión se justifica como un medio más de control».

35. Esta afirmación merece ser matizada, pues será perfectamente conocedor de la información aparente, no de la que se pueda extraer de archivos que creía borrados, historial de navegación, etc.

36. El propio RDPJ prevé en el segundo párrafo de su artículo noveno la creación de unidades con ámbito territorial superior al provincial «por razones de especialización delictual o de técnicas de investigación».

37. Castillejo Manzanares, «Alguna de las cuestiones que plantean las diligencias de investigación tecnológica», *Revista de derecho y proceso penal*, núm. 45, 2017, *ob. cit*, p. 34.

38. Véase Sánchez Gómez, «El agente encubierto informático», en *La ley penal: revista de derecho penal, procesal y penitenciario*, vol. 4, núm. 118, 2016 págs. 1 a 25.

ritmos aplicados para la identificación de los mismos, lo que permitirá la posterior entrada en el domicilio de investigado y la incautación de los dispositivos con los que se sospecha que desarrolla su actividad delictiva.

2. Letrado de la Administración de Justicia

La norma no prevé la presencia del LAJ durante el registro de los dispositivos, lo que ha dado lugar a que casi todos los autores que han escrito sobre esta diligencia hayan tratado esta cuestión. La jurisprudencia anterior a la nueva regulación venía señalando que, durante el volcado, como mera copia de datos de un dispositivo a otro, se hacía innecesaria la presencia del LAJ; esta línea ha ido consolidándose con el paso de los años[39] y es perfectamente aplicable a la situación actual tras la Ley Orgánica 13/2015, de 5 de octubre. En los supuestos de registros con ocasión de una entrada domiciliaria, sí estará el LAJ presente, aunque aquello no supondrá necesariamente que este vaya a estar presente durante el volcado, pues puede diferirse su realización, limitándose la entrada y registro a la incautación. Anteriormente, se expuso que es unánime en la doctrina la alta conveniencia de la presencia del LAJ para garantizar la autenticidad de las copias y que, aunque no existe un procedimiento reglado para el desarrollo de la diligencia[40], todos los autores que proponen procedimientos coinciden en que, de una forma u otra, debe intervenir garantizando la autenticidad de los datos.

El hecho de que la norma guarde silencio respecto a la intervención del LAJ no significa que esta no pueda llegar a ser obligatoria. Dependerá de la resolución que dicte el juez de instrucción. La LECrim le impone al juez la obligación de fijar «las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación» y los términos en los que se practique la diligencia, por lo que dentro del diseño que haga caso por caso de la intervención podrá fijar momentos puntuales en los que la presencia sea obligatoria y este deba levantar acta. Esto debe enlazarse con lo dispuesto en el artículo 588 bis.k.1 de la LECrim, dentro de las disposiciones comunes, que regula la destrucción de los registros e impone la obligación de conservar de copia del registro bajo custodia del LAJ. Esta previsión funcionará de distinta forma en esta medida, pues, de todas ellas, solamente el registro de dispositivos de almacenamiento de datos requiere la realización de copias desde el inicio. Imponiendo la LECrim que en todo caso deba existir una copia bajo custodia del LAJ, carecería de sentido que la copia que le llegue al LAJ sea remitida a través de los investigadores y sin la garantía de autenticidad que sí se tendría en caso de haberse obtenido la copia de forma inicial y en su presencia. Por ello, aunque tanto se ha escrito respecto a la no obligatoriedad de la presencia del LAJ durante la realización de copias, entiendo que esta obligación viene derivada de la puesta en relación de las especificidades de esta medida con la exigencia del artículo 588 bis.k.1 de la LECrim.

3. El investigado y su defensa

Aunque este punto tampoco ha sido regulado por la norma, es evidente su relevancia. La regla general será que el investigado se encuentre presente durante el momento de la incautación de los dispositivos y la realización de la copia si esta se realiza en el mismo acto ya que, en caso de registro domiciliario, el investigado habrá de estar presente (art. 569 de la LECrim) y en los demás casos será al investigado al que se le incauten directamente los dispo-

39. La STS 507/2020, de 14 de octubre, cita a su vez la STS 116/2017, de 23/02/2017:
«No es discutible que la ruptura de la cadena de custodia puede tener una indudable influencia en la vulneración de los derechos a un proceso con todas las garantías y a la presunción de inocencia. De ahí que coincidamos con el recurrente cuando enfatiza su importancia desde la perspectiva de las garantías del proceso penal. Resulta imprescindible descartar la posibilidad de que la falta de control administrativo o jurisdiccional en las fuentes de prueba pueda generar un equívoco acerca de la autenticidad de los datos bancarios luego valorados. Lo contrario podría implicar una más que visible quiebra de los principios que definen el derecho a un proceso justo.
Pues bien, la defensa condiciona la admisión de la autenticidad de esos archivos a unos presupuestos que en nada condicionan nuestra valoración. De una parte, lamenta que el volcado de esos datos, con carácter previo a su remisión a las autoridades españolas, se produjera sin intervención judicial. Sin embargo, mal puede exigirse a las autoridades francesas lo que ni siquiera es exigible en el territorio jurisdiccional español. En efecto, conviene recordar que la jurisprudencia de esta Sala no ha considerado que la práctica de las operaciones técnicas de volcado exija como presupuesto de validez, no ya la presencia del Juez, sino la presencia misma del Secretario judicial (cfr. SSTS 324//2013, 17 de julio; 480/2009, 22 de mayo; 256/2008, 14 de mayo y 15 noviembre 1999 -recaída en el rec. núm. 3831/1998). Lo decisivo es que queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto del registro e intervención de los ordenadores y la que se obtiene mediante el volcado».

40. La regulación de la medida en la LECrim prácticamente se agota en los requisitos de la resolución judicial, dejando el desarrollo en manos del juez de instrucción en la fijación del término y alcance de la medida.

sitivos, teniendo siempre en estos casos la posibilidad de participar, colaborar, efectuar manifestaciones o negarse a todo ello. Caso distinto serán aquellos supuestos como el analizado en la SAP Barcelona 255/2019, de 6 de mayo, en donde es un tercero el que hace entrega de los dispositivos. Ya se expuso en el apartado relativo al término y alcance del registro que ha venido sosteniéndose, tanto por diversos autores como por la FGE, que la intervención del investigado es necesaria en los supuestos en los que se realicen copias lógicas a fin de que durante el proceso de selección de archivos no se le cause indefensión, permitiéndosele la contradicción en la selección de elementos a analizar. Cuando se realicen copias idénticas no parece razonablemente argumentable la necesidad de la presencia del investigado, al menos desde la perspectiva del derecho de defensa.

En lo que respecta al letrado del investigado, la LECrim no prevé su presencia en ningún momento durante la diligencia, únicamente siendo necesaria en casos en los que el investigado esté detenido y este deba prestar su consentimiento, tal como prevé desde el año 2015 el art. 520.6.c de la LECrim y venía requiriendo la jurisprudencia con anterioridad. Será el juez de instrucción en la resolución que fije las garantías para la realización de la diligencia el que diseñe un procedimiento con intervención del letrado o no, siendo conveniente que se encuentre presente en todas aquellas fases de la diligencia en las que se requiera algún tipo de actuación por parte del investigado. Realmente no existen razones para exigir que el investigado se encuentre asesorado antes de prestar su consentimiento para la medida cuando está detenido y no en el resto de casos. Según el art. 520.6.c de la LECrim, el fundamento es que el investigado conozca las consecuencias del consentimiento[41], no otras, y no cabe duda de que las consecuencias del consentimiento serán las mismas, tanto si está detenido como si no: se accederá a su entorno virtual y la información que se busque o casualmente se encuentre podrá ser utilizada en su contra. Siendo las consecuencias de la prestación del consentimiento las mismas en un caso que en otro, quizá sería conveniente arbitrar mecanismos para garantizar que quienes prestan su consentimiento para el registro de sus dispositivos conozcan previamente las posibles consecuencias de su asentimiento. No parece razonable exigir asistencia letrada para la prestación del consentimiento en todo caso, pero no debería ser admisible que un individuo sea requerido por la policía para mostrar o entregar el contenido de sus dispositivos sin haber sido informado previamente de su derecho a oponerse y de la posibilidad de que todo lo que sea hallado pueda ser utilizado en contra suya. Cabe recordar, por último, que las circunstancias ambientales en las que una persona presta su asentimiento a la exigencia de los agentes policiales pueden dar lugar a que el juez declare inválido el consentimiento otorgado[42].

4. El deber de colaboración

Dentro del apartado destinado a las personas que participan durante la ejecución de la diligencia no podía faltar la referencia a aquellas personas que por imperativo legal deben participar de forma activa, son aquellas obligadas por el llamado «deber de colaboración». Regulado en el art. 588 sexies.c.5 de la LECrim, este deber surge en el momento en que las autoridades y agentes encargados de la investigación ordenan a quienes conocen el funcionamiento del sistema informático o las medidas para proteger los datos alojados en ellos, que faciliten el acceso a los investigadores, so pena de incurrir en delito de desobediencia. Las únicas excepciones a este deber son: a) que la carga que supondría la colaboración con los agentes fuese desproporcionada; b) ser el investigado; c) estar amparado por el secreto profesional y d) ser alguna de las personas a las que la LECrim dispensa de la obligación de declarar por razón de parentesco.

IV. LOS DATOS OBTENIDOS EN EL PROCEDIMIENTO PENAL

Una vez que se ha obtenido copia de los dispositivos de interés para la investigación y se ha procedido a su análisis, dos grandes dudas surgen sobre qué hacer con la información obtenida: 1) cómo incorporar esta a la causa, y

41. Art. 520.6.c de la LECrim:
«6. La asistencia del abogado consistirá en:
(…)
c) Informar al detenido de las consecuencias de la prestación o denegación de consentimiento a la práctica de diligencias que se le soliciten».

42. En el apartado relativo al consentimiento se citaba la SAP Madrid 353/2020, de 24 de septiembre, en la que se declara nulo el consentimiento prestado por el factor intimidatorio del entorno en el que fue prestado, rodeado de tres agentes de policía que le daban órdenes a las que el investigado no se opuso.

2) qué información es la que debe tener entrada en la causa y, en su caso, cómo proceder al expurgo de información irrelevante.

1. Incorporación

Una vez que se obtiene la copia del contenido del dispositivo de almacenamiento de datos y se accede a los mismos, los resultados del registro deben poder entrar al procedimiento penal. Siguiendo a Delgado Martín[43] en su distinción entre «fuente/medio de prueba en el mundo digital», por un lado, estará el medio en el que se contenga el archivo digital (la fuente de prueba), cuya autenticidad e integridad quedará más o menos salvaguardada según el diseño de garantías que haya previsto el juez de instrucción en la autorización de la medida y del que se podrán extraer los ficheros de interés; y, por otro, el medio a través del cual dar entrada en la causa a la información contenida en los ficheros (el medio de prueba), señalando el autor que, en principio, todos los medios de prueba previstos en el art. 299 de la LEC «son aptos para incorporar al proceso los datos electrónicos»[44] y que las partes procesales deberán elegir un medio u otro «teniendo en cuenta la posición procesal que eventualmente puede adoptar la parte contraria» en atención a eventuales impugnaciones[45].

Apunta Magro Servet[46] que «la parte que desee proponer una prueba digital ante el juez instructor deberá identificar la fuente de la prueba para llevar al proceso el instrumento donde está la digital. No obstante, en muchas ocasiones, la fuente de prueba no es algo físico que se pueda presentar y/o aportar», lo que llevará a «tener que preconstituir la prueba digital para poder hacerla valer más tarde, siendo preciso que el legislador pueda recoger los medios, modos y formas por los que se puede preconstituir la prueba digital que es más fácil que otras que "desaparezca", lo que podemos hacer con anticipación de la prueba digital por medio del examen inmediato por el juez y levantarse acta judicial de lo que existe en ese medio digital, adveración por el letrado de la Administración de Justicia, o acta notarial respecto a lo que el notario comprueba y la ubicación en donde ese contenido concreto se encuentra», no necesitando de documentación aquellas pruebas también de carácter digital susceptibles de ser visionadas en juicio oral «como puede ser una grabación de imagen o sonido», que únicamente requerirá que la sala de vistas cuente con medios para su reproducción[47].

La información contenida en los dispositivos de almacenamiento deberá acceder a la causa de alguna de estas formas, a lo que deberá añadírsele que en el caso de la diligencia prevista en los arts. 588 sexies a) de la LECrim y ss., se elaborarán informes técnicos policiales con la consideración de informes periciales[48]. Según Gudín Rodrí-

43. Delgado Martín, «¿Cómo afrontar la complejidad de la prueba digital?», *Derecho Digital e Innovación. Digital Law and Innovation Review*, núm. 2, 2019. Wolters Kluwer.

44. Debe recordarse que el art. 299 de la LEC prevé determinados medios de prueba convencionales, pero abre la puerta a que tengan entrada al proceso otros medios de prueba distintos a los previstos, previendo el art. 299.2 de la LEC que sean los propios «instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas» los que tengan entrada al procedimiento. El artículo los incluye dentro de la regulación de los medios de prueba y su admisión lo será como tal (no como fuente de prueba), pero no parece posible que los datos puedan entrar en la causa si no es mediante interrogatorios, testificales, periciales, documentos o reconocimiento judicial; siendo plenamente consciente el legislador de la situación actual de la prueba digital, prevé en el art. 384 de la LEC (en relación con el 382.2 de la LEC) la aportación de «dictámenes y medios de prueba instrumentales» para poder introducir los datos incluidos en archivos dentro del procedimiento, así como para hacer valer la autenticidad y exactitud de los archivos.

45. Según el autor, las implicaciones de la impugnación —o no impugnación— son muy distintas en la jurisdicción civil y en la penal. En la civil, «la falta de impugnación por aquel a quien perjudique determina un supuesto de prueba tasada: el documento hará prueba plena en el proceso en los mismos términos que los documentos públicos»; mientras que «[e]ste carácter de prueba tasada resulta difícilmente admisible en el proceso penal, de tal manera que la misma habrá de ser valorada por el Juez en relación con otros elementos de conformidad con la sana crítica ex art. 741 LECRIM. Otra cosa es que dicha falta de impugnación pueda facilitar la eficacia probatoria del documento».

46. Magro Servet, «¿Cómo aportar la prueba digital en el proceso penal?», *Diario La Ley*, núm. 9824, 2021.

47. Para lo que será recomendable aportar este medio de prueba con suficiente antelación a la celebración del juicio oral y no proponer la prueba al comienzo de las sesiones (art. 786.2 de la LECrim), a fin de evitar que la misma no pueda ser practicada por carecer la sala medios para la reproducción de audio y sonido.

48. Apunta también Portal Manrubia que en aquellos casos en que el agente que proceda a la incautación y volcado de los dispositivos sea el mismo que quien elabore posteriormente el informe, dicho agente podrá deponer tanto como testigo como perito. Así, en Portal Manrubia, «La incorporación de los dispositivos de almacenamiento masivo en el procedimiento penal». *Revista Aranzadi Doctrinal*, núm. 2, 17, 2019, *ob. cit*, expone el autor que «[e]stos informes no se encuentran regulados de manera expresa en nuestra legislación procesal penal, siendo probable que el informe pericial sea emitido por quien realice la clonación de los datos digitales. Dicho sujeto actúa en el procedimiento penal de testigo, al aportar conocimientos propios y responder sobre las reacciones que los investigados o terceros presentaban mientras la incautación o el proceso de clonado se materializaba, y también de perito, al contribuir con conocimientos especializados».

guez-Magariños[49], los peritos, «adoptando las medidas y garantías adecuadas para preservar el contenido de la información pueden proceder a la extracción de la información más relevante atendiendo a los criterios de búsqueda facilitados por el equipo investigador», permitiendo su análisis «la recuperación de los archivos ocultos, restableciendo los vínculos suprimidos y recabando los metadatos que permitirán reconstruir el origen de la información, la identidad del delincuente y las circunstancias y el tiempo de la creación, modificaciones, y de las distintas versiones del archivo». Los informes contendrán el resultado del análisis de los archivos, pero no servirán por sí mismos para acreditar el contenido del mismo, que deberá ser valorado por el juez o tribunal en el acto del juicio oral, siendo esencial que los documentos, audios, imágenes o vídeos sean debidamente aportados al procedimiento. También podrán ser elaboradas periciales por encargo de las partes, normalmente las defensas, a fin de poder poner en tela de juicio la autenticidad e integridad de los datos.

Otro medio de prueba que se ha señalado a través del cual poder incorporar la prueba digital es el reconocimiento judicial. De esta cuestión se ha ocupado Arrabal Platero[50] indicando que «[e]l reconocimiento judicial es un medio apto para incorporar evidencias tecnológicas a través de la percepción directa del juez de datos de prueba, como son el acceso desde el ordenador del Juzgado a una determinada página web, el examen judicial de los correos electrónicos remitidos desde una dirección de email o la exploración del contenido de un ordenador (…). El problema, no obstante, puede darse en relación con la posible alteración de una prueba tecnológica —piénsese una página web— previamente al reconocimiento judicial. Una posible solución es, en primer lugar, que la prueba tecnológica se asegure previamente a través del hash» y «recurrir a páginas web que almacenan registros del histórico de los cambios de otras páginas web y que permiten consultar el contenido de una página web en una fecha concreta, como *Wayback Machine*». También señala la autora que podrá determinarse mediante reconocimiento judicial «la autoría de las voces de una grabación de audio o de las conversaciones intervenidas e incorporadas al acervo probatorio a través de otro medio de prueba, sin necesidad de un dictamen pericial sobre su autoría o del reconocimiento del acusado sobre las mismas», postura que viene respaldada por la jurisprudencia. Esto último puede ser peligroso para las garantías procesales y derechos fundamentales del acusado, pues el hecho de que el juzgador, que no posee conocimientos científicos sobre la materia, pueda efectuar esta determinación de la autoría de las voces, si no viene de la mano de una exhaustiva labor de motivación probatoria, será susceptible de vulnerar tanto su derecho a la tutela judicial efectiva como su derecho a la presunción de inocencia en caso de condena[51].

2. Expurgo

En la regulación del registro de dispositivos de almacenamiento de datos no se prevé la posibilidad de limitar qué datos acceden a la copia del dispositivo que pueden solicitar las partes, siendo así que en muchos casos habrá información absolutamente irrelevante e innecesaria que llegue a las demás partes del procedimiento, incluso información que pertenece en exclusiva a la vida íntima y personal del investigado. Esto, por el contrario, sí está previsto en la LECrim para la interceptación de las comunicaciones telefónicas y telemáticas:

> **Artículo 588 ter i. Acceso de las partes a las grabaciones.**
>
> «1. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso.
>
> 2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

49. Gudín Rodríguez-Magariños, «Incorporación al proceso del material informático intervenido durante la investigación penal», *Boletín del Ministerio de Justicia*, vol. 68, núm. 2163, 2014, pp. 17-18.

50. Arrabal Platero, *La prueba tecnológica aportación, práctica y valoración*, Tirant lo Blanch, 2020, pp. 309-310.

51. STS 224/2022, de 9 de marzo (F.J.2.º):
«La vulneración del derecho a la tutela judicial efectiva en el aspecto relativo a la motivación probatoria de la sentencia de condena, puede ocasionar igualmente una vulneración de la presunción de inocencia».

ISSN: 2951-844X

3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia».

Propone Arrabal Platero[52] la inclusión de «una disposición común a todas las diligencias de investigación tecnológica que prevea un trámite para la incorporación de información que, aunque haya sido excluida, la parte la considere notoria o ayude a la valoración del conjunto (como en la actualidad está previsto para la intervención de las comunicaciones) y para el expurgo de la información obtenida que sea irrelevante para la causa o cuya afectación a derechos fundamentales de particulares no sea proporcional a su interés», estimando «necesario disponer de un trámite que posibilite excluir información innecesaria, ajena al objeto de la causa que, además, afecte a un interés jurídicamente tutelado —por ejemplo, la imagen de la víctima, la seguridad, el patrimonio o el honor de las personas—, o aquélla en la que intervengan menores; y, coetáneamente, que permita incorporar aquella otra información que sirva a los efectos de una correcta interpretación de las ya aportadas».

El juez de instrucción, al fijar los términos y el alcance del registro y las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación, puede diseñar un trámite para el expurgo de la información contenida en los dispositivos. Esto es posible a causa de la insoportable renuncia a regular esta materia que efectuó el legislador en 2015, no pudiendo entenderse que la misma reforma de la LECrim cree un procedimiento para el expurgo de información en supuestos de intervenciones telefónicas y no lo prevea para supuestos en los que se realizan copias de los ordenadores personales y teléfonos móviles del investigado; reforma que, como se ha venido apuntando desde el inicio, se llevó a cabo en busca de aumentar garantías para la preservación del derecho del investigado a la exclusión de su entorno virtual. En el caso de elaboración de copias lógicas quizá no sea necesaria esta cautela, pero en el de las copias idénticas sí, pues no debería permitirse que todas las partes obtengan una copia íntegra de los dispositivos del investigado. Así, los jueces de instrucción, aprovechando que todas las medidas de investigación tecnológica se sustancian en pieza separada, deberán arbitrar mecanismos para que a la pieza principal únicamente acceda la información relevante. No es tarea sencilla la de diseñar un procedimiento para el expurgo de información, pues deben garantizarse tanto los derechos del afectado como el de los demás coimputados y partes acusadoras, debiendo haber sido el legislador quien diseñase el procedimiento a fin de evitar que en cada juzgado de instrucción de España se prevea un sistema de salvaguarda de derechos fundamentales distinto.

V. A MODO DE CONCLUSIÓN

La LECrim se preocupa de en qué casos puede producirse la autorización o convalidación de la incautación y registro de dispositivos, así como qué principios inspiran la medida. Sobre cómo debe realizarse la medida, la norma guarda silencio, quizá debiendo haber sido algo más exhaustivo el legislador. En la regulación actual, deberá ser el juez de instrucción el arquitecto de la medida de investigación. El diseño de la diligencia que se realice en el auto autorizante será el que determine la forma de realizarse el análisis y las garantías de integridad y autenticidad de los datos. Atendiendo a lo que se ha venido señalando por diversos autores, será recomendable que se pronuncie sobre:

a) Si han de realizarse copias idénticas o copias lógicas.
b) La presencia e intervención del LAJ.
c) La presencia e intervención del investigado y su defensa.
d) Un eventual y recomendable procedimiento de expurgo.

Respecto al contenido de la copia del dispositivo analizado, la fuente de prueba entrará en el procedimiento, a través un informe de análisis técnico policial, como prueba documental o por medios de reproducción de palabras, imagen y/o sonido. Los demás medios de prueba servirán para reforzar el resultado obtenido.

52. Arrabal Platero, La incorporación al proceso de las evidencias obtenidas de equipos informáticos y de dispositivos de almacenamiento masivo de información. El expurgo del contenido irrelevante, *Revista Aranzadi de derecho y nuevas tecnologías*. N.º 56, 2021.

VI. BIBLIOGRAFÍA

Arrabal Platero, «La incorporación al proceso de las evidencias obtenidas de equipos informáticos y de dispositivos de almacenamiento masivo de información. El expurgo del contenido irrelevante», *Revista Aranzadi de derecho y nuevas tecnologías.* N.º 56, 2021.

Arrabal Platero, *La prueba tecnológica aportación, práctica y valoración*, Tirant lo Blanch, 2020.

Castillejo Manzanares, «Alguna de las cuestiones que plantean las diligencias de investigación tecnológica», *Revista de derecho y proceso penal*, núm. 45, 2017, pp. 23–57.

Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.

Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre sobre registro de dispositivos y equipos informáticos.

Delgado Martín, «¿Cómo afrontar la complejidad de la prueba digital?», *Derecho Digital e Innovación. Digital Law and Innovation Review*, núm. 2, 2019, Wolters Kluwer.

Delgado Martín, «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por la LO 13/2015», en *Diario La Ley*, 2016, núm. 8693, pág. 12 y ss.

Fernández-Gallardo, «Registro de dispositivos de almacenamiento masivo de información», *Dereito revista xurídica da Universidade de Santiago de Compostela*, vol. 25, núm. 2, 2016, pp. 25–58.

Gómez Colomer, «Los actos de investigación garantizados», en *Derecho Jurisdiccional III. Procesal Penal* (con Montero Aroca, Esparza Leibar, Barona Vilar, Etxeberría Guridi), Tirant Lo Blanch, Valencia, 2016, págs. 262 y ss.

Gudín Rodríguez-Magariños, «Incorporación al proceso del material informático intervenido durante la investigación penal», *Boletín del Ministerio de Justicia*, vol. 68, núm. 2163, 2014.

Gudín Rodríguez-Magariños, «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información», *La ley penal: revista de derecho penal, procesal y penitenciario*, 2017, núm. 125, págs. 16 y ss.

Magro Servet, «¿Cómo aportar la prueba digital en el proceso penal?», *Diario La Ley*, núm. 9824, 2021.

Martínez Atienza, *Investigación tecnológica en los ciberdelitos*, Ediciones Experiencia, 2020.

Pérez Estrada, «La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información», *Revista Brasileira de Direito Processual Penal*, vol. 5, núm. 3, 2019, págs. 1297–1330.

Portal Manrubia, «La incorporación de los dispositivos de almacenamiento masivo en el procedimiento penal», *Revista Aranzadi Doctrinal*, núm. 2, 2019.

Ruiz Legazpi, «Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (incoming de eMule) en la STC 207/2011», *Revista española de derecho constitucional*, vol. 34, núm. 100, 2014, págs. 365–390.

Sánchez Gómez, «El agente encubierto informático», *La ley penal: revista de derecho penal, procesal y penitenciario*, vol. 4, núm. 118, 2016.

Sánchez Gómez, *El derecho de defensa en la investigación de los delitos de terrorismo*. Aranzadi, 2017.

SÁNCHEZ GÓMEZ, «El tratamiento integral de la entrada y el registro en el marco del proceso penal, Wolters Kluwer, Madrid, 2021, págs. 168 y ss.

SÁNCHEZ GÓMEZ, «La investigación tecnológica multinivel del discurso terrorista», *La represión y persecución penal del discurso terrorista* (Galán Muñoz, dir., Gómez Rivero, dir.), Tirant lo Blanch, 2022, págs. 761-801.