Circular 5/2019, *sobre registro de dispositivos y equipos informáticos*

1. Introducción

Entre las medidas de investigación tecnológica a las que la Ley Orgánica 13/2015, de 5 de octubre, *de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, ha dado entrada en la Ley de Enjuiciamiento Criminal (en adelante, LECrim) no podía faltar el registro de los dispositivos y sistemas informáticos. Efectivamente, la informática se ha convertido en los últimos años, no ya en una parte importante de la vida de las personas, sino en el centro en torno al cual gravitan numerosas actividades cotidianas en las sociedades modernas.

Ese protagonismo adquirido por la informática se ha dejado sentir, también, en el modo en el que se desarrollan numerosos comportamientos delictivos que, o bien recaen directamente sobre los dispositivos o sistemas informáticos, provocando así el nacimiento de nuevas formas de delito, o bien utilizan la informática como medio

o instrumento privilegiado para su desarrollo. Precisamente por esto, en los últimos años el uso de la informática ha resultado también capital para la persecución del delito. Ambas circunstancias constituyen el motivo esencial de la irrupción progresiva de la informática en el proceso penal, no ya como instrumento de trabajo, sino como objeto y medio de prueba y, al mismo tiempo, como medio de investigación de los delitos.

Esta situación, en buena medida huérfana de regulación legal, es la que ha venido a abordar en profundidad la LO 13/2015 y, entre las medidas que regula, ocupando un lugar destacado, el registro de dispositivos y sistemas informáticos.

El punto de partida de esta regulación y que da sentido a la misma aparece recogido en el Preámbulo de la Ley 13/2015, cuando descarta que los dispositivos de almacenamiento masivo de información puedan ser considerados como simples piezas de convicción. Su capacidad para recoger y conservar datos de muy diferente índole permite que el acceso a los mismos pueda llegar a afectar de manera intensa a diversos derechos fundamentales y, de ahí, la naturaleza y exigencias de la regulación legal. Esta idea, ya reconocida por la jurisprudencia, deriva de la consideración de los ordenadores como algo más que un *instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad del usuario* (STS nº 342/2013, de 17 de abril).

La nueva regulación ha venido a dar cumplimiento a diversas exigencias internacionales, como la que recogía el art. 19 del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE de 17 de septiembre de 2010), que señalaba: “Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar: a) A un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio”. Ya antes, incluso, se venía poniendo de relieve en diversos instrumentos internacionales la grave afectación de

la intimidad que podía derivar del acceso inconsentido a datos informáticos almacenados, como ocurría en el Convenio núm. 108 del Consejo de Europa de 28 de Enero de 1981, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* o en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)*; se llegaba a hablar ya de la necesidad de control judicial en cualquier clase de medida de vigilancia informática, como en la Resolución del Parlamento Europeo de 17 de diciembre de 1998, *sobre el respeto de los derechos humanos en la Unión Europea* (apartado 23).

La regulación legal del registro de dispositivos y sistemas informáticos, por lo demás, venía siendo demandada, igualmente, por los Tribunales al resultar evidente la trascendencia que para la tutela de los derechos fundamentales podía suponer la protección del contenido almacenado (en este sentido, STC nº 173/2011, de 7 de noviembre).

Al abordar el registro de dispositivos o equipos informáticos, el legislador ha optado por distinguir entre un registro estático, el de los dispositivos de almacenamiento masivo de información, y un registro dinámico, el registro remoto sobre equipos informáticos que, si bien presentan numerosas notas comunes, también ofrecen aspectos singulares que invitan a su tratamiento independiente. Toda la regulación que ahora se establece, además, estará siempre presidida por las disposiciones comunes de aplicación general a todas las diligencias de investigación tecnológica que se recogen en el Capítulo IV del Título VIII del Libro II LECrim que han sido objeto de análisis en la Circular 1/2019.

2. Derecho fundamental afectado

Tradicionalmente, la doctrina jurisprudencial venía considerando que en el registro de dispositivos o sistemas informáticos podían verse comprometidos dos diferentes

derechos fundamentales. Con carácter general, se entendía que se afectaba la intimidad del usuario del dispositivo, ya que todos los datos que es posible almacenar en el mismo (en forma de documentos, carpetas, fotografías, vídeos, etc.) son susceptibles de "afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc." (STC nº 173/2011, de 7 de noviembre). Pero, al mismo tiempo, podían también derivarse limitaciones para el derecho fundamental al secreto de las comunicaciones si el registro del dispositivo (ordenador o teléfono móvil, por ejemplo) alcanzaba a datos almacenados que formaran parte de procesos comunicativos. A esta distinción aludía la Circular 1/2013, de 11 de enero, *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, señalando que "lo determinante para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE no es el tipo de soporte, físico o electrónico, en el que la agenda de contactos esté alojada ni el hecho de que la agenda sea una aplicación de un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se accede".

La distinción en el tratamiento del registro de los contenidos de esta clase de dispositivos generaba no pocos problemas en atención al diferente grado de exigencia que ambos derechos fundamentales requerían para su limitación: autorización judicial en el caso del art. 18.3 CE y no necesidad de la misma en el del art. 18.1 CE. Así, por ejemplo, se venía distinguiendo una diferente naturaleza a los mensajes de correo electrónico según que hubiesen sido ya leídos o no, al entenderse que el proceso comunicativo había finalizado ya en el primer caso y no así en el segundo, no resultando precisa autorización judicial para su incautación en un caso y sí en el otro (STS nº 864/2015, de 10 de diciembre). Igualmente, se distinguía entre el registro de la agenda de contactos de un teléfono móvil, no necesitada de autorización judicial (STC nº 115/2013, de 9 de mayo) y la revisión del registro de llamadas entrantes y salientes que, por afectar al derecho fundamental al secreto de las comunicaciones, precisaba de autorización judicial (STC nº 230/2007, de 5 de noviembre).

La solución al problema vino dada por el nacimiento de una nueva doctrina jurisprudencial que abordaba de manera unitaria el problema, introduciendo el concepto del “derecho al entorno virtual” como un derecho omnicomprensivo que abarca la protección de la gran diversidad de datos que pueden guardarse en un dispositivo o sistema informático, como puede ser un ordenador. De esta manera, señalaba la STS nº 342/2013, de 17 de abril: “la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual”.

Efectivamente, como expresa la STC nº 173/2011, de 7 de noviembre, “quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona”.

Piénsese, por ejemplo, que cualquier persona conserva actualmente en su teléfono móvil información sobre todos sus contactos (personales y profesionales), su agenda, con información acerca de sus hábitos más íntimos, sus mensajes de correo electrónico y mensajería instantánea, fotografías familiares, íntimas o relacionadas con secretos profesionales, la geolocalización que resulte de las rutas o desplazamientos que haya realizado en los últimos meses (o años), etc. Por eso,

el registro de alguno de los actuales dispositivos de almacenamiento, como los ordenadores o los *smartphones* o teléfonos inteligentes, puede suponer una intromisión en los derechos fundamentales del individuo que supere ampliamente la limitación aislada de cada uno de los derechos comprometidos, justificando de esta manera su tratamiento unitario para, de esta forma, llevar a cabo una ponderación y valoración, también unitaria, de los derechos e intereses que pudieran resultar comprometidos.

Así lo reconocía ya la citada STS nº 342/2013, de 17 de abril, cuando señalaba que en el derecho al entorno virtual 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". Esta resolución pone de relieve "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".

Pero es que, además, el tratamiento unitario de los derechos comprometidos resulta necesario para garantizar la eficacia de un eventual registro, en atención a la gran diversidad de datos y archivos que pueden encontrarse en un dispositivo o sistema informático. Así, no sería extraño que se autorizase el acceso a datos íntimos amparados por el art. 18.1 CE y, en el curso del registro, aparecieran comunicaciones relevantes para la investigación amparadas por el art. 18.3 CE (STS nº 204/2016, de 10 de marzo). Por ello, la autorización para el registro de un dispositivo o sistema informático en la que se habilite para el acceso a la totalidad del entorno virtual de su usuario, evitará que puedan surgir problemas derivados de la naturaleza del contenido que pudiera ser hallado.

Este es el fundamento de la nueva regulación que incorpora la LO 13/2015. El registro de dispositivos de almacenamiento masivo de información o de equipos o sistemas informáticos se regirá ahora por las previsiones que la LECrim contiene

para esta clase de diligencias. Resultará innecesario, por lo tanto, plantearse si resulta comprometido el derecho a la intimidad o el secreto de las comunicaciones. La nueva regulación legal encomienda ahora al Juez valorar -normalmente con carácter previo, aunque, en algunos supuestos con posterioridad al registro, como se verá- la procedencia de la medida en el caso concreto, teniendo en cuenta que, con ella, como se ha señalado, los poderes públicos accederán a ese entorno virtual constitucionalmente protegido del que es titular el investigado. Como expresa la STS nº 786/2015, de 4 de diciembre, "la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo". Solo a la hora de motivar específicamente la medida deberá descenderse al análisis particular de los derechos controvertidos, cuyo mayor o menor protagonismo y afectación, determinarán la mayor o menor exigencia de los principios rectores que habrán de presidir la medida.

3. Registro de dispositivos de almacenamiento masivo de información

3.1. Regulación legal

El Capítulo VIII, del Título VIII, del Libro II, LECrim, aparece dedicado al *registro de dispositivos de almacenamiento masivo de información.* Comprende tres preceptos (arts. 588 sexies a a 588 sexies c), a lo largo de los cuales se condensa toda la regulación que, igual que ocurre con el resto de diligencias de investigación tecnológica, aparece complementada por las Disposiciones Comunes que se incluyen en el Capítulo IV de este mismo Título (arts. 588 bis a a 588 bis k).

Al analizar la aplicación de estos preceptos no debe desconocerse, igual que ocurre en relación con otras medidas de investigación tecnológica, que la regulación que la LECrim recoge quedará circunscrita a los supuestos que la justifican en atención a su encuadramiento sistemático dentro de la propia Ley; en particular, de la rúbrica que encabeza el Título VIII *-De las medidas de*

investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución- se desprende que los preceptos que se analizan resultarán únicamente aplicables a aquellos registros de dispositivos de almacenamiento masivo de información que sean acordados por las autoridades públicas en la persecución de delitos, pudiendo resultar afectados los derechos reconocidos en el art. 18 CE.

Así, por ejemplo, quedarán excluidos del ámbito de la regulación los accesos a dispositivos de almacenamiento masivo de información llevados a cabo por particulares en contextos desconectados de la investigación de los delitos. En este sentido, proclama la STS nº 287/2017, de 19 de abril: "se trata de una prueba proporcionada por un particular a los agentes de la autoridad sin que esa entrega haya sido concebida como un mecanismo de elusión de las garantías que el sistema constitucional reconoce para la protección de los derechos a la intimidad y al entorno virtual. Hemos dicho que "… las reglas de exclusión probatoria se distancian de su verdadero sentido cuando no tienen relación con la finalidad que está en el origen mismo de su formulación. De lo que se trata es de limitar el afán del Estado en la persecución de los ilícitos penales, de apartar a los agentes de la autoridad de la tentación de valerse de medios de prueba que, por su alto grado de injerencia en el círculo de los derechos fundamentales, están sometidos a unas garantías constitucionales concebidas para la salvaguardia de aquéllos. Se ha dicho con acierto que la proscripción de la prueba ilícita se explica por el efecto disuasorio que para el aparato oficial del Estado representa tener plena conciencia de que nunca podrá valerse de pruebas obtenidas con vulneración de las reglas constitucionales en juego". En este mismo sentido, el ejercicio de la patria potestad por los padres les confiere también a estos una facultad de control sobre la intimidad de sus hijos menores que puede traducirse en el acceso y registro legítimo de sus datos íntimos, pudiendo llegar a generar prueba valorable por un Tribunal, no obstante su obtención al margen de la previsión legal (STS nº 864/2015, de 10 de diciembre).

Igualmente quedarían excluidos de la regulación los supuestos de registro de dispositivos que, por el objeto y fines para los que se utilizan, resultaran extraños al ejercicio del derecho a la intimidad por particulares. Es el caso de la STS nº 426/2016, de 19 de mayo, que señala que "no obstante lo anterior en el caso presente no se trata de despachos, ni ordenadores privados del recurrente sino de los existentes en un organismo público como es la Jefatura Provincial de Tráfico, que no ampara la intimidad que protege el domicilio y quienes trabajan en ellos y los utilizan por razón de su trabajo, no tienen una pretensión de privacidad que el lugar no les puede proporcionar". La falta de expectativa razonable de privacidad constituye también el argumento del Tribunal Constitucional (STC nº 170/2013, de 7 de octubre) para no considerar vulnerados los derechos fundamentales de un trabajador cuyo ordenador fue intervenido y registrado por la empresa.

De manera congruente con la regulación del resto de las medidas de investigación tecnológica, el legislador parte de los criterios generales ya establecidos en el Capítulo IV, para precisar en este Capítulo VIII las especialidades que presenta esta medida en relación con otras.

3.2. Los dispositivos de almacenamiento masivo de información

Los dispositivos de almacenamiento de datos pueden ser definidos como la unión de una serie de componentes que tienen la capacidad de escribir, conservar y posteriormente recuperar o leer datos en un soporte de almacenamiento. A diferencia del soporte de almacenamiento de datos, que sería simplemente el material físico donde se escriben y almacenan esos datos, en el dispositivo de almacenamiento existen diversos componentes, no solo el soporte donde se graba la información, sino también los dispositivos que la escriben y leen, formando todo ello una unidad. Así, por ejemplo, sería un soporte de almacenamiento de datos un disco DVD, mientras que el dispositivo de almacenamiento vendría constituido por la unidad de DVD, esto es, lo que se conoce como grabadora de DVD.

Los dispositivos de almacenamiento masivo de información a que hacen referencia los arts. 588 sexies a a 588 sexies c LECrim comprenderán, no solo los instrumentos capaces de grabar, almacenar y posteriormente recuperar o leer información digital, sino también los soportes empleados para ello y que carecen de funcionalidad sin el dispositivo que en ellos escribe o lee.

Los dispositivos que hoy en día se utilizan de manera generalizada pueden agruparse en tres grandes categorías: dispositivos magnéticos (fundamentalmente, unidades de disco duro o HDD, del inglés *Hard Disk Drive*), dispositivos ópticos (CD, DVD o BD) y los dispositivos de memoria sólida o SSD (acrónimo inglés de *solid-state drive*) (tarjetas de memoria, memorias USB, etc.)

Podría inducir a confusión la enumeración que recoge el precepto, al hacer referencia a los ordenadores e instrumentos de comunicación telefónica o telemática, que sitúa en un plano de igualdad con los dispositivos de almacenamiento masivo de información digital. En realidad, tanto los ordenadores como los instrumentos de comunicación telefónica o telemática son tecnologías que contienen y hacen uso de dispositivos de almacenamiento masivo de información digital, pero, aun siendo los más frecuentemente utilizados, no son los únicos. Son, igualmente, instrumentos que contienen y utilizan dispositivos de almacenamiento masivo de información, las tabletas (a mitad de camino entre el ordenador personal y el teléfono inteligente), las cámaras fotográficas, los GPS o incluso numerosos electrodomésticos de uso cotidiano hoy en día que permiten grabar y almacenar información de diversa naturaleza.

Por lo tanto, lo que la regulación legal autoriza a registrar será, además de los ordenadores y teléfonos móviles expresamente mencionados, cualquier otro dispositivo de almacenamiento masivo que forme parte de otro instrumento más complejo -como los anteriormente reseñados-, así como los soportes de almacenamiento de datos que puedan ser hallados (como CD´s ó DVD´s) y los dispositivos de almacenamiento masivo de información que, sin formar parte de otro sistema más complejo, pudieran tener relación con la investigación (discos

duros externos, memorias USB, tarjetas de memoria, etc.) A ello deberá añadirse, además, el acceso a cualquiera de estos dispositivos o instrumentos por vía telemática, esto es, lo que la ley llama el acceso a repositorios telemáticos de datos.

Finalmente, es preciso hacer mención, también, a lo que la regulación legal llama instrumentos de comunicación telemática, que serían todos aquellos dispositivos que, de algún modo, intervengan en las comunicaciones a distancia que puedan tener lugar a través de medios informáticos. Aunque realmente aquí se incluirán, de manera principal, los ordenadores y los teléfonos móviles, recogidos específicamente en la previsión legal, la regulación alcanzaría también a otros dispositivos, como los enrutadores (más conocidos como *routers*, por su denominación en inglés) que, al tiempo que facilitan las comunicaciones telemáticas, pueden proporcionar interesantes datos a una investigación criminal.

3.3. La resolución judicial como presupuesto de la medida

3.3.1. La resolución judicial habilitante

Como se ha señalado, con anterioridad a la reforma operada por LO 13/2015 existía una jurisprudencia consolidada que entendía que la habilitación judicial previa para el registro de un dispositivo de almacenamiento masivo de información, como un teléfono móvil inteligente, dependía del derecho fundamental que se pudiera ver comprometido. De esta manera, cuando se trataba del secreto de las comunicaciones se exigía siempre previa autorización judicial, pero no así cuando era simplemente la intimidad del investigado la que podía resultar limitada por el registro, como ocurría en los casos de inspección de la agenda de contactos de un teléfono móvil. La reforma procesal ha puesto fin a esta situación, incorporando casi textualmente al articulado de la LECrim el art. 347 de la Propuesta de Código Procesal Penal de 2013, que ya introducía la exigencia de autorización judicial necesaria en todos los casos de registro de esta clase de dispositivos.

La necesidad del control judicial de esta medida ya había sido puesta de manifiesto por el TEDH (STEDH de 22 de mayo de 2008, caso Iliya Stefanov contra Bulgaria) y, más recientemente, por el Tribunal Supremo de Estados Unidos que, en su sentencia de 25 de junio de 2014 (casos acumulados Riley contra California y Estados Unidos contra Brima Wurie -573 U.S.- 2014), destacaba la gravísima afectación de la privacidad que podía derivarse de un examen indiscriminado y sin límites de un teléfono inteligente. En esta línea, como ya se señalaba, la STS nº 342/2013, de 17 de abril, acogía en nuestro país el concepto del derecho al propio entorno virtual para justificar esa necesidad de autorización judicial, precisando la STS nº 246/2014, de 2 de abril, ante la diferente naturaleza de los derechos que pueden verse afectados por el registro de un ordenador: “Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal”.

Efectivamente, la diversa naturaleza de los datos que pueden ser almacenados en un dispositivo digital se traduce, también, en diferentes grados de afectación de los derechos fundamentales de su titular, lo que impone un tratamiento unitario que permita salvaguardar las intromisiones que pudieran resultar más intensas (en este sentido, la STS nº 204/2016, de 10 de marzo).

Pues bien, esa multifuncionalidad de los datos que se almacenan y el diferente grado de afectación de los derechos fundamentales del investigado, no solo justifica la exigencia de una resolución judicial para su registro, sino que también constituye el núcleo y la esencia de la fundamentación que debe recoger esa autorización judicial. Deberá valorarse el alcance del registro, la naturaleza de los datos a los que se accederá y el grado de afectación de los derechos del investigado, como criterio fundamental para llevar a cabo una adecuada ponderación de los intereses en conflicto que justifique el registro. De esta manera, las exigencias de justificación se incrementarán en los casos en los que pueda

presumirse la limitación de diversos derechos fundamentales (intimidad, secreto de las comunicaciones o protección de datos) o cuando, aun siendo solo uno el derecho afectado, se prevea de especial intensidad su afectación (por ejemplo, cuando se trate de datos pertenecientes al ámbito más exclusivo de la privacidad). Por el contrario, la justificación podrá no ser tan intensa cuando se trate de acceder a datos concretos y limitados que no incidan de manera especialmente grave en el derecho fundamental (por ejemplo, el simple acceso al directorio de contactos de un teléfono móvil).

En cualquier caso, no debe olvidarse que la menor exigencia de justificación que se derive de las circunstancias concretas de cada supuesto no podrá traducirse nunca en la inobservancia de alguno de los principios rectores que el art. 588 bis a recoge entre sus disposiciones generales, que deberán siempre concurrir en su totalidad; todo lo más, en los casos de menor afectación de los derechos fundamentales, se exigirá una menor intensidad en las exigencias derivadas de esos principios rectores.

El principio de especialidad, en estos casos, va a hacer que no resulte lícito el registro preventivo o genérico de dispositivos (como podría ser un teléfono móvil, por ejemplo) sin que exista una investigación sobre un delito concreto. Esta circunstancia, unida a las exigencias del principio de excepcionalidad, debe traducirse en la ilegalidad de cualquier registro de dispositivos que se llevara a cabo de manera sistemática ante cualquier detención, por ejemplo. La excepcionalidad de la medida deberá ser apreciada juntamente con su idoneidad y necesidad. Por ello, solo ante la posibilidad indiciariamente acreditada de obtener con el registro datos relevantes para la investigación, podría justificarse el mismo. Por lo tanto, el registro resultará ilícito cuando se lleve a cabo de manera prospectiva, esto es, buscando el hallazgo casual de datos o pruebas que, a priori, no aparezcan justificados.

Finalmente, y en cuanto a la proporcionalidad de la medida, pudiera llamar la atención que el legislador no haya establecido un catálogo de delitos fijando una

gravedad mínima que permita el recurso a esta medida, si se tiene en cuenta la importancia de la intromisión en los derechos fundamentales que con ella puede producirse. La razón de ello estriba en que, frente a esa gravedad que se presenta en algunos casos concretos, existen otros, como ya se adelantaba, mucho más livianos. Por ello, deberá ser el juicio de proporcionalidad que lleve a cabo el Juez el que justifique la medida en cada caso concreto; y ese juicio deberá valorar la gravedad del delito, no solo desde la perspectiva de la pena que le corresponda, sino atendiendo también a la naturaleza del bien jurídico protegido.

Especial significación alcanzará, en estos casos, el ámbito tecnológico en el que el delito se haya cometido, ya que únicamente mediante el análisis del medio tecnológico de comisión podrán reunirse pruebas de su perpetración. En este sentido, señala la STS nº 811/2015, de 9 de diciembre, que "cuando de infracciones cometidas mediante la utilización de equipos informáticos se trata, la diligencia tendente a su ocupación y al examen de sus contenidos, ha de considerarse como proporcionada, no tanto en función de la pena eventualmente aplicable sino de la propia naturaleza de los hechos investigados, de su mecánica comisiva y de las inevitables necesidades para su ulterior probanza".

De todas formas, no debe olvidarse que la menor gravedad de la infracción puede compensarse, desde la perspectiva de la proporcionalidad, con una limitación de los datos a los que se permite el acceso. Así, mientras que una simple estafa de escasa cuantía no justificaría el pleno acceso a la totalidad de los datos íntimos del investigado que pudiera almacenar en su ordenador personal, no existiría inconveniente en considerar proporcionada la autorización judicial que concediera acceso a su actividad en internet, si este hubiera sido el medio de comisión del delito.

3.3.2. El consentimiento del afectado y otros supuestos excepcionales

La autorización judicial habilitante del registro de un dispositivo de almacenamiento masivo de información no será necesaria en los casos en los que el afectado haya

prestado su consentimiento para ello. Aunque no lo prevea expresamente la Ley, la eficacia del consentimiento sobre el derecho a la intimidad ha sido objeto de un intenso desarrollo jurisprudencial; de esta manera, el Tribunal Constitucional, en STC nº 173/2011, de 7 de noviembre, proclamaba que "corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, por lo que el consentimiento del titular del derecho fundamental legitimará la inmisión en el ámbito de la intimidad e impedirá, por tanto, considerarlo vulnerado".

Será siempre presupuesto necesario para la validez del consentimiento que el otorgante tenga capacidad para prestarlo, proclamando la STS nº 1803/2002, de 4 de noviembre que "en supuestos de minusvalía psíquica aparente, esté o no declarada judicialmente, no puede considerarse válidamente prestado el consentimiento, todo ello en base al art. 25 del Código Penal".

Podrá manifestarlo el afectado, tanto de manera expresa como tácita, entendiéndose por ésta última la que no resulta *de expresiones, sino de hechos (actos concluyentes), siendo preciso, para conocer su verdadero significado, acudir a conjeturas o presunciones* (STC nº 173/2011, de 7 de noviembre). El propio art. 551 LECrim se refiere al consentimiento para la práctica de la diligencia de entrada y registro señalando que "se entenderá que presta su consentimiento aquel que, requerido por quien hubiere de efectuar la entrada y registro para que los permita, ejecuta por su parte los actos necesarios que de él dependan para que puedan tener efecto, sin invocar la inviolabilidad que reconoce al domicilio el artículo 6.º de la Constitución del Estado" (actual art. 18.2 Constitución Española).

Ahora bien, no puede admitirse como un consentimiento tácito la simple falta de oposición al registro (en este sentido la STC nº 209/2007, de 31 de septiembre, respecto de un registro domiciliario) siendo preciso, al menos, actos que manifiesten una inequívoca voluntad de colaborar con ese registro como sería, por ejemplo, el supuesto recogido en la STS nº 786/2015, de 4 de diciembre, en el que se admitió que esa voluntad tácita se dedujera del acto de facilitar la interesada la

identidad de las cuentas de correo electrónico y sus claves. La STS nº 864/2015, de 10 de diciembre, por su parte, consideró válido el consentimiento tácito para el análisis de un ordenador que se desprende de la autorización a la policía para recogerlo, considerando "incuestionable que la autorización para recoger conlleva el análisis del contenido que en dicho material informático se encuentre". Finalmente, puede recordarse también el caso de la STC nº 173/2011, de 7 de noviembre, en la que se entiende prestado el consentimiento con la entrega de un ordenador que carece de contraseñas, para el acceso al mismo con el fin de que sea reparado.

El consentimiento podrá ser revocado en cualquier momento (SSTC nº 196/2006, de 3 de julio y 159/2009, de 29 de junio) y, además, devendrá ineficaz cuando el registro "subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (SSTC nº 110/1984, de 26 de noviembre, 196/2004, de 15 de noviembre y 70/2009, de 23 de marzo). Igualmente, el consentimiento ha de ser libre y no viciado ya que, como señala la STS nº 1576/1998, de 11 de diciembre, "ha de estar exento de todo elemento susceptible de provocar o constituir error, violencia, intimidación o engaño (art. 1.265 del Código Civil), pues si tales rigurosas exigencias son requeridas para las relaciones contractuales, mucha más severidad habrá de aplicarse cuando se trata de renunciar a un derecho fundamental del individuo". En esta línea, no debe olvidarse que el último apartado del art. 588 sexies c prohíbe expresamente a las autoridades y agentes encargados de la investigación que puedan compeler al investigado o encausado para que colabore en el registro del dispositivo.

En los casos en los que el afectado se encuentre detenido, aplicando la doctrina jurisprudencial elaborada para los casos de registro domiciliario, no será precisa la asistencia del letrado para llevar a cabo el registro del dispositivo, pero sí para obtener el consentimiento del afectado, si no existiera autorización judicial (STS nº 187/2014, de 10 de marzo). "La razón de ello -señala la STS 550/2001, de 3 de abril-, es que la manifestación de voluntad así prestada debe ser seriamente

cuestionada teniendo en cuenta que el detenido puede sentirse condicionado o presionado por dicha situación, incluso desconocer la posibilidad de negarse a autorizar la entrada, así como las consecuencias que pudieran derivarse de dicho acto". Esta misma asistencia letrada para la eficacia del consentimiento en los casos de detención se viene exigiendo para la validez de la toma de muestras biológicas (SSTS nº 685/2010, de 7 de julio y 827/2011, de 25 de octubre) (art. 520.6.c) LECrim).

Existen otros supuestos, no obstante, en los que el consentimiento para el registro presenta alguna particularidad. Es el caso, por ejemplo, del registro de dispositivos de almacenamiento que son utilizados simultáneamente por varias personas, en el que resultará válido el consentimiento otorgado por cualesquiera de ellas, incluso, para el examen de los datos íntimos de las otras. A él se refiere la STS nº 287/2017, de 19 de abril, referido al registro de un ordenador utilizado por todo el entorno familiar con el simple consentimiento de uno de los miembros; señala el Tribunal Supremo que "quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable". El consentimiento de uno de los usuarios, sin embargo, no deberá resultar suficiente cuando pudiera existir conflicto de intereses entre ellos (STC nº 22/2003, de 10 de febrero). En los casos de datos íntimos de una persona fallecida, aunque en este caso se trataba de la víctima del delito, la STS nº 850/2014, de 26 de noviembre, valida el consentimiento de sus padres para acceder a los datos existentes en su teléfono móvil, señalando: "Desde la perspectiva del derecho a la intimidad, no constituye una injerencia inconstitucional el acceso proporcional de los padres de la menor fallecida, en su condición de sucesores legítimos en todos sus bienes, derechos y obligaciones, a sus documentos privados. Y desde la perspectiva del derecho al secreto de las comunicaciones (…) los sucesores legítimos del receptor, titulares de todos sus derechos y obligaciones, pueden asimismo acceder y hacer un uso legítimo y proporcionado de dichas comunicaciones, sin por ello vulnerar ningún precepto constitucional".

3.3.3. La resolución judicial en los supuestos de registros domiciliarios

El caso que con mayor frecuencia se presenta en relación con el registro de dispositivos de almacenamiento masivo de información es el de su incautación como consecuencia de la realización de una diligencia de entrada y registro. Con anterioridad a la reforma de la LECrim, 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 documentos del mismo que pudieran tener relación con el delito. La nueva regulación, sin embargo, parte de la conclusión esencial de que la simple incautación de los dispositivos de almacenamiento masivo de información que se lleve a cabo con motivo de una entrada y registro no permite acceder al contenido de los mismos. Es decir, la autorización judicial de entrada y registro permite la incautación de los dispositivos (*efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación*, dice el art. 546 LECrim), pero será necesaria una motivación judicial especial e independiente para registrar o acceder a la información contenida en los dispositivos.

A esta necesidad se refiere la STS nº 786/2015, de 4 de diciembre, cuando señala: “La jurisprudencia de esta Sala ha recordado la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del derecho al entorno digital de todo investigado. Como hemos indicado supra, esa resolución ha de tener un contenido propio, explicativo de las razones por las que, además de la inviolabilidad domiciliaria, se alza la intimidad reflejada en el ordenador. Nuestro sistema no tolera el sacrificio de los derechos proclamados en los apartados 3 y 4 del art. 18 de la CE a partir de una legitimación derivada, de suerte que lo que justifica un sacrificio se ensanche hasta validar implícitamente otra restricción. Esta idea tiene ya un reflejo normativo en el art. 588 sexies a) 1º de la LECrim (…) Se trata, por tanto, de una regulación rupturista, que pretende abandonar prácticas en las que la autorización judicial para la entrada en el domicilio del investigado amparaba

cualquier otro acto de injerencia, incluso cuando desbordara el contenido material del derecho reconocido en el art. 18.2 de la CE".

La motivación judicial que legitime el registro de los dispositivos de almacenamiento puede realizarse en la misma resolución de entrada y registro o en otra independiente (SSTS nº 342/2013, de 17 de abril y 204/2016, de 10 de marzo). Lo normal será que, tanto la motivación que justifique el registro domiciliario, como la que justifique el registro de los dispositivos de almacenamiento, se incluyan en la misma resolución judicial en los casos en los que sea previsible el hallazgo de esta clase de dispositivos y su relevancia para la investigación con anterioridad a la práctica de la diligencia (art. 588 bis a.1), aunque nada impide que esa justificación se realice por separado. Cuando necesariamente constarán ambas justificaciones en resoluciones diferentes será en los supuestos que prevé el apartado 2 del art. 588 sexies a, en los que el auto de entrada y registro habrá legitimado la incautación de los dispositivos, pero resultará necesaria una nueva resolución, con su motivación específica, para su registro. Realmente, hoy en día es difícil imaginar un registro domiciliario en el que no aparezca algún tipo de dispositivo de almacenamiento masivo de información por lo que, siempre que se considere que pudiera resultar relevante para la investigación que se lleva a cabo la información que en uno de estos dispositivos pudiera ser almacenada, deberá preverse específicamente en el auto de entrada y registro el acceso a la misma.

Es necesario que la justificación del registro de los dispositivos de almacenamiento masivo tenga un contenido propio e independiente del que habilita el registro domiciliario. Como declara la STS nº 786/2015, de 4 de diciembre, lo que la Ley pretende "es que el Juez de instrucción exteriorice de forma fiscalizable las razones que justifican la intromisión en cada uno de los distintos espacios de exclusión que el ciudadano define frente a terceros". Esta circunstancia podría determinar, incluso, la nulidad de una de las diligencias y no de la otra, al estar sujetas ambas a exigencias distintas; por eso, en los supuestos en los que las dos motivaciones judiciales se incluyan en una misma resolución, deberá prestarse un especial cuidado con el fin de fundamentar la procedencia de cada una de ellas.

De la distinción entre ambas diligencias de investigación deriva, al mismo tiempo, la consecuencia de que no puedan extenderse al registro de los dispositivos las exigencias que se establecen para los registros domiciliarios. Así, aunque para el registro del domicilio será necesaria la presencia del interesado en los términos previstos por la LECrim, no lo será para el acceso a la información del dispositivo. Este diferente tratamiento, además, viene impuesto por la naturaleza de uno y otro registro; mientras que el registro de un domicilio puede desarrollarse en unas pocas horas, el de un dispositivo de almacenamiento masivo de información puede prolongarse durante días o incluso semanas.

3.3.4. Incautación de dispositivos fuera del domicilio

El art. 588 bis b se encarga de precisar que la autorización judicial para el registro de dispositivos de almacenamiento masivo de información será también necesaria cuando estos hayan sido incautados *con independencia de un registro domiciliario.* Se tratará de supuestos en los que, por ejemplo, con motivo de una detención -o sin necesidad de ésta-, la Policía ocupe el teléfono móvil de un sospechoso o el dispositivo de geolocalización de un vehículo implicado en un grave accidente o, en definitiva, el ordenador del investigado en un hecho delictivo.

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. Así, por ejemplo, cuando se vaya a proceder a la detención de una persona respecto de la que existan sospechas de que porta un teléfono móvil con información relevante para la causa, nada impediría que, en el propio auto de detención o con independencia a este, se resolviera y motivara adecuadamente la procedencia de registrar su teléfono.

La iniciativa para el registro -e incluso para la incautación- de dispositivos de almacenamiento masivo de información no tiene por qué partir necesariamente de la Policía, pese a que el precepto parece darlo por supuesto. Al contrario, podrá el Juez, de oficio o a solicitud del Ministerio Fiscal, acordar la incautación y registro o únicamente el registro, si se trata de dispositivos ya incautados.

Para concluir, es preciso poner de relieve que la autorización judicial que regula el precepto lo es solo para el registro o análisis del contenido del dispositivo, pero no para su aprehensión o incautación, que no precisa autorización judicial previa. De esta manera, cuando se trate de la Policía Judicial, la recogida de los efectos, instrumentos o pruebas del delito, constituirá uno de sus cometidos y, al propio tiempo, obligaciones (art. 282 LECrim). El Juez, por su parte, puede también ordenar la recogida de efectos o pruebas materiales conforme a lo previsto en el art. 326 LECrim.

3.4. Alcance del registro

El art. 588 sexies c, en sus dos primeros apartados, aborda el análisis de cuatro aspectos esenciales para la eficacia de los registros de dispositivos de almacenamiento masivo de información: la necesidad de que la resolución judicial precise los términos y el alcance del registro, la posibilidad de realización de copias de los datos informáticos, la necesaria fijación de las condiciones para asegurar la preservación e integridad de los datos y la conveniencia de evitar la incautación de los soportes de almacenamiento salvo excepciones.

3.4.1. Fijación de los términos y alcance del registro

La LECrim impone al Juez la obligación de precisar *los términos y alcance del registro*, esto es, los concretos datos informáticos a los que podrá acceder la investigación. Esta decisión deberá estar presidida por los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Se trata de garantizar que la limitación de los derechos fundamentales del afectado alcance

únicamente hasta donde resulte estrictamente necesario a los fines de la investigación, garantizando, al propio tiempo, el respeto al resto de su entorno virtual.

La delimitación del alcance del registro que debe hacer el Juez tendrá una proyección tanto subjetiva como objetiva. Subjetiva, porque deberá precisar los sujetos afectados por el registro; aunque ordinariamente resultará solo afectado el investigado, el registro podría limitar derechos de terceros si el dispositivo de almacenamiento masivo es compartido entre varias personas o si los datos de interés para la investigación se encuentran almacenados en dispositivos que no son titularidad del investigado. Esa posible afectación de terceros aparece ya prevista en los arts. 588 bis c.3.b) y 588 bis h LECrim para todas las medidas de investigación tecnológica, por lo que cabe remitirse a las precisiones que sobre este particular se hacían en la Circular 1/2019. Además, la posibilidad de registrar dispositivos de un tercero parece admitida por la regulación específica de esta medida, cuando habla de “titular o propietario” en el art. 588 sexies c.2. Pero, sobre todo, la delimitación que haga el Juez debe tener un alcance objetivo, no solo determinando qué dispositivos pueden ser registrados y cuáles no, sino, también, la categoría o clase de datos o archivos de un dispositivo determinado a los que deberá alcanzar el registro.

El Juez, por lo tanto, partiendo de la naturaleza del delito que se investiga y de la clase de datos que se pretenda obtener con el registro deberá precisar en la resolución habilitante tanto los dispositivos que serán objeto de registro como la naturaleza o categoría de los datos que podrán ser registrados o, desde una perspectiva negativa, la naturaleza o categoría de los datos a los que no deberá alcanzar el registro.

Ahora bien, existen supuestos en los que la delimitación de los términos y alcance del registro no resultará sencilla. Esto puede ocurrir cuando se investiguen comportamientos delictivos capaces de generar registros informáticos de distinta naturaleza. Sería el caso, por ejemplo, de la investigación de delitos complejos,

como el tráfico de drogas y blanqueo de capitales, que exigiría registrar la práctica totalidad de los datos almacenados (comunicaciones, datos económicos, fotografías, vídeos…). Otro tanto ocurriría en el caso de la investigación de delitos especialmente graves, en los que el principio de proporcionalidad podría justificar una intromisión más relevante en el conjunto de datos que conforman el entorno digital de una persona y que, indiciariamente, pudieran resultar relevantes para una investigación por ser de uso frecuente en las dinámicas delictivas, como sucede, por ejemplo, en los casos de terrorismo. Finalmente, la adopción de especiales cautelas por parte de los investigados puede determinar que se amplíe el ámbito del registro en busca de archivos intencionadamente camuflados entre las ingentes cantidades de información que pueden almacenarse en uno de estos dispositivos, como podría ocurrir, por ejemplo, en los casos de criminalidad organizada. En todos estos supuestos, la investigación policial previa a la incautación de los dispositivos deberá orientarse, entre otros fines, a determinar los indicios que posteriormente puedan sustentar un determinado alcance del registro.

Aunque puede no resultar sencillo delimitar los términos y alcance de un registro en un caso concreto, el acierto de la medida pasará siempre por una adecuada justificación de los límites fijados, se revelen posteriormente como correctos o no. Por ello, lo realmente determinante para la validez de la medida, lo que hará que la misma resulte ajustada a derecho, será siempre que la resolución habilitante haya fijado un determinado alcance del registro -que podrá ser de todo el dispositivo o de parte del mismo-, y que, al mismo tiempo, haya reflejado las razones y motivos en los que descansa esa decisión. A partir de aquí, será la razonabilidad o no del juicio valorativo, lo que dará validez o no a la decisión judicial.

Así, la STEDH, de 3 de julio de 2012, caso Robathin contra Austria, consideró violado el art. 8 de la Convención Europea de Derechos Humanos (en adelante, CEDH) en un supuesto de registro del ordenador de un abogado en el que la medida había permitido el acceso a todos los datos y no únicamente a las carpetas referidas a los clientes que eran objeto de investigación. El fundamento de la resolución, sin embargo, no fue el excesivo alcance del registro, sino la falta de

justificación de ese alcance, señalando el TEDH que el Tribunal “dio razones muy breves y bastante generales al autorizar la búsqueda de todos los datos electrónicos del bufete de abogados del solicitante. En particular, no abordó la cuestión de si sería suficiente buscar solo los discos que contenían datos relacionados con "R." y "G." Tampoco dio ninguna razón específica para su conclusión de que era necesaria una búsqueda de todos los datos del solicitante para la investigación”.

Por otro lado, determinado un concreto alcance del registro en la resolución judicial, sin embargo, nada impide que los términos fijados puedan ser ampliados en una nueva resolución si, como consecuencia del registro iniciado, apareciesen indicios que justifican la necesidad de acceder a otros datos.

Para concluir, es preciso señalar que la delimitación del alcance del registro también puede venir determinada por la concreta técnica que se utilice. De esta manera, que se autorice a investigar realizando búsquedas en la totalidad de los datos almacenados en un concreto dispositivo no significa que se vaya a acceder a la intimidad de todos esos datos. Efectivamente, existen herramientas forenses que utilizan motores de búsqueda que permiten hallar determinados archivos en un ordenador o sistema informático sin necesidad de mostrar el contenido de todos los archivos sobre los que realiza la búsqueda. De esta forma, la privacidad del afectado queda salvaguardada, no obstante el análisis de todos sus archivos.

3.4.2. Realización de copias

El apartado primero del art. 588 sexies c establece que la resolución judicial podrá autorizar la realización de copias de los datos informáticos, lo que parece contradictorio con la previsión contenida en el apartado segundo del mismo artículo, que impone la realización de las copias como regla general, evitando la incautación de los soportes de almacenamiento. Teniendo en cuenta que la realización de copias será el modo habitual de proceder, la previsión legal deberá interpretarse en el sentido de que la realización de copias requerirá siempre la

autorización del Juez. Si bien es cierto que el copiado de los dispositivos constituye un mecanismo esencial para garantizar la integridad de la prueba, también lo es que supone una intromisión mayor en el entorno virtual del afectado que su simple visualización, de ahí que la ley prevea expresamente la necesidad de autorizar la copia.

Efectivamente, la volatilidad y facilidad de alteración de los datos informáticos aconsejan, con la finalidad de garantizar la integridad de la prueba, que el registro y análisis de los dispositivos de almacenamiento se practique sobre copias y no sobre los originales. La realización de copias permitirá, igualmente, un mayor dinamismo en la elaboración de informes sobre el contenido de los dispositivos, al poder realizarse simultáneamente diversos estudios sobre los mismos (en los casos en los que vayan a ser examinados por los peritos designados por el Juez y, al propio tiempo, por otras partes intervinientes).

El copiado de dispositivos de almacenamiento masivo de información puede llevarse a cabo de dos formas. Mediante el clonado o volcado, que consiste en la realización de una copia espejo o copia bit a bit de la información original, o mediante la realización de una copia lógica, es decir, una copia selectiva de ciertas carpetas o ficheros. En el primer caso, la imagen obtenida con la copia será idéntica a la original (hasta en los archivos que hayan podido ser borrados del soporte de almacenamiento) y debe ser firmada digitalmente a través de una función *hash*, que garantizará la identidad de los datos informáticos entre los que existen en la copia y el original. En el caso de las copias lógicas, sin perjuicio de que también es posible la firma digital a través de la función *hash*, sería recomendable su realización a presencia del Letrado de la Administración de Justicia con el fin de otorgar mayores garantías a la selección de archivos que se copien.

La copia autorizada por el Juez puede llevarse a cabo al mismo tiempo que se practica el registro del domicilio o lugar en el que el dispositivo de almacenamiento haya sido hallado, o posponerse para un momento ulterior. La primera solución

aporta agilidad a la investigación, al poderse utilizar esas copias ya desde un primer momento, pero presenta el inconveniente de que el proceso de copiado puede resultar bastante lento y prolongarse más allá de lo que dure el registro domiciliario, sobre todo, en los casos de clonado. Por eso, la práctica más habitual consistirá en la incautación de los dispositivos de almacenamiento masivo de información en el momento del registro domiciliario para su posterior clonado. Por el contrario, cuando se acuerde realizar copias lógicas durante el registro domiciliario deberá aprovecharse la presencia del Letrado de la Administración de Justicia para que haga constar en el acta del registro el concreto alcance del copiado del dispositivo, garantizándose con ello la autenticidad e integridad de la copia en virtud de las cautelas que adopte el Letrado de la Administración de Justicia. En la práctica serán las concretas circunstancias del caso, su urgencia o la naturaleza de los datos que interesen a la investigación, las que aconsejen decantarse por uno u otro tipo de copiado.

A diferencia de lo que se ha señalado para la realización de copias lógicas o parciales, durante el volcado o clonado de datos no es necesaria la presencia del Letrado de la Administración de Justicia (SSTS nº 116/2017, de 23 de febrero, 342/2013, 17 de julio, 480/2009, 22 de mayo y 256/2008, 14 de mayo). Como se ha indicado, la garantía de la integridad de la copia vendrá dada en estos casos por la firma digital (al poderse comprobar que el resultado de la función hash del original coincide exactamente con el de la copia). La función del Letrado de la Administración de Justicia, en estos casos, se agotará en dar fe de la identidad del soporte de almacenamiento masivo de información, esto es, que el soporte copiado es el mismo que fue hallado en el registro domiciliario y, como tal, consignado en el acta. En este sentido, señala la STS nº 342/2013 más arriba citada: “la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica. Lo decisivo es que, ya sea mediante la intervención de aquél durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado”. Por otro lado, el

proceso de volcado o clonado se lleva a cabo a través de un procedimiento técnico que el Letrado de la Administración de Justicia no solo puede desconocer, sino que, además, no siempre puede controlar, por lo que difícilmente podrá dar fe del mismo: “aunque no hay duda de que el secretario judicial es una instancia formal de garantía, la jurisprudencia aconseja no sobrevalorar su mediación, por su propia condición de profano en materia de conocimientos informáticos” (STS nº 187/2015, de 14 de abril). Añade la STS nº 1599/99, de 15 de noviembre: “Lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia”.

Ahora bien, aunque la intervención del Letrado de la Administración de Justicia no sea necesaria durante el proceso de copiado, en ocasiones será preciso que garantice la identidad e integridad de la prueba extendiendo acta en el momento de desprecinto del dispositivo y comienzo del clonado, así como de la conclusión del mismo. Igualmente, en los supuestos excepcionales en los que en el proceso de clonado concurran circunstancias extraordinarias que pudieran suscitar dudas acerca de la identidad o integridad de la prueba, deberá proponerse su intervención.

Cosa diferente es lo que ocurre en los casos de realización de copias lógicas, en los que, como se indicaba, 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. En cualquier caso, no debe olvidarse que el copiado de los datos es una cuestión de legalidad ordinaria que no alcanza a afectar a los derechos fundamentales, por lo que las irregularidades que puedan producirse en su práctica se traducirán en la imposibilidad de valorar la prueba, pero no en su nulidad, con las consecuencias que de ello derivan.

La presencia del interesado, en principio, no es necesaria para llevar a cabo el copiado de los datos. En los supuestos en los que se practique durante la diligencia de entrada y registro, sin embargo, su presencia en el propio registro debe permitirle presenciar el copiado. Además, 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.

El art. 336 LECrim reconoce al afectado y su Letrado el derecho de asistir al reconocimiento pericial de efectos que pudieran tener relación con el delito. En el caso de los dispositivos de almacenamiento masivo de información, dicha facultad debe interpretarse como la posibilidad de que el afectado designe su propio perito para llevar a cabo otro reconocimiento pericial distinto, ante la imposibilidad de admitir una interpretación literal del precepto en este caso, en atención a la duración del largo proceso de análisis de esta clase de dispositivos.

Finalmente, respecto a la posibilidad de que las partes asistan al acto de volcado o clonado de los dispositivos de almacenamiento señala la STS nº 165/2016, de 2 de marzo, que “ni la ley procesal anterior al año 2015 ni tampoco la nueva normativa de la Ley de Enjuiciamiento Criminal (Ley 13/2015, de 5 de octubre) imponen que estén presentes el letrado del imputado ni un perito nombrado por la parte en el momento de volcar el contenido del ordenador”. Es cierto que el art. 476 LECrim reconoce a las partes la posibilidad de designar un perito que presencie el acto pero, sin embargo, “esa presencia no es presupuesto de validez del acto. Nada de ello se desprende de la literalidad de aquel precepto” (STS nº 342/2013, de 17 de abril).

3.4.3. Fijación de las condiciones para asegurar la integridad de los datos y las garantías de su preservación

Además de precisar el alcance del registro y decidir acerca de la realización o no de copias, la resolución judicial deberá también fijar las *condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial* (art. 588 sexies c). No precisa la Ley, sin embargo, las condiciones y garantías concretas que hayan de adoptarse, por lo que deberá estarse a las reglas generales acerca de la conservación y garantía de las fuentes de prueba.

A pesar de que el precepto parece condicionar la finalidad de asegurar la integridad de los datos y su preservación a la hipotética práctica de un dictamen pericial, debe interpretarse que las medidas que adopte el Juez deberán estar orientadas, en último término, a garantizar la integridad y preservación de los datos para su adecuada valoración por el Tribunal de enjuiciamiento, no solo en los casos en que exista prueba pericial, sino también en los de valoración del dato directamente por el Tribunal. Se trata, en definitiva, de garantizar la adecuada cadena de custodia de las fuentes de prueba, asegurando que lo que se *analiza es justamente lo ocupado y que no ha sufrido alteración alguna* (STS nº 1072/2012, de 11 de diciembre). Y es que, en cualquier caso, la aptitud de la prueba pericial va a pasar siempre por garantizar la adecuada cadena de custodia de los efectos objeto de la pericia, asegurando que son los mismos y con el mismo contenido, que los que fueron intervenidos (STC nº 170/2003, de 29 de septiembre).

Estas condiciones que el Juez habrá de fijar en su resolución deberán pasar, necesariamente, por garantizar la identidad de los dispositivos de almacenamiento masivo (que los dispositivos de los que nacen las pruebas son los mismos que fueron incautados) y su integridad (que no se ha borrado ni añadido dato alguno en los mismos).

El medio idóneo e imprescindible para garantizar la identidad de los dispositivos incautados será su adecuada reseña por el Letrado de la Administración de Justicia en el acta del registro cuando el dispositivo haya sido incautado con motivo de éste. En los demás casos, como podría ser, por ejemplo, la incautación con motivo de una detención policial, deberá la Policía Judicial identificar adecuadamente en el acta que al efecto se levante y que deberá figurar unida al atestado que se presente, el dispositivo incautado. Igualmente, en los casos de ocupación de los dispositivos con motivo de un registro, será necesario observar cautelas especiales para garantizar la identidad de los datos cuando se trate de registros en despachos de abogados. Así lo impone la jurisprudencia del TEDH, que exige la presencia del decano o representante del colegio profesional o equivalente (STEDH de 23 de noviembre de 2010, caso Moulin contra Francia).

Para garantizar la integridad de los dispositivos resultará necesario su adecuado precinto y puesta a disposición judicial en el momento de su incautación. Cualquier posterior apertura del precinto, como sería la necesaria para llevar a cabo el clonado del dispositivo, deberá hacerse bajo la fe del Letrado de la Administración de Justicia; una vez realizado el clonado, el dispositivo deberá ser nuevamente precintado. Igualmente, la integridad del contenido del dispositivo exige que el clonado se lleve a cabo a través de instrumentos y programas que respeten plenamente el contenido del soporte que va a ser copiado, no realizando alteración alguna en el mismo. Es, precisamente, esta necesidad de garantizar la integridad e identidad del contenido de los dispositivos de almacenamiento masivo de información, la que aconseja realizar siempre los análisis sobre copias y no sobre el soporte original. Esto permitirá que, ante la sospecha de manipulación de la copia, se cuente siempre con el original intacto para garantizar su contenido.

No obstante lo anterior, en los supuestos en los que no se incaute el dispositivo, dejándolo en poder del investigado, será preciso hacer dos copias; una primera, para garantizar y asegurar el contenido del dispositivo en un momento determinado y una segunda para llevar a cabo sobre ella los análisis que exija la investigación, dejando de esta manera intacta y como muestra de contraste la primera copia,

cuya integridad será garantizada por el sellado y custodia de la misma que deberá hacer el Letrado de la Administración de Justicia.

Las condiciones fijadas por el Juez para la integridad y preservación de los datos pueden ser cuestionadas por las partes, no solo en el momento de su adopción, sino también cuando se revelen ineficaces o se incumplan, aunque siempre precisando concretamente el déficit de garantía y haciéndolo en un momento procesal que permita su corrección. En este sentido, señala la STS nº 990/2016, de 12 de enero: “Para examinar adecuadamente si se ha producido una ruptura relevante de la cadena de custodia no es suficiente con el planteamiento de dudas de carácter genérico, es necesario que la parte que la cuestione precise en qué momentos, a causa de qué actuaciones y en qué medida se ha producido tal interrupción, pudiendo proponer en la instancia las pruebas encaminadas a su acreditación. En cualquier caso, habrá de plantearse en momento procesalmente hábil para que las acusaciones, si a su derecho interesa, puedan contradecir eficazmente las objeciones planteadas”. Esto es así porque “existe la presunción de (que) lo recabado por el juez, el perito o la policía se corresponde con lo presentado el día del juicio como prueba, salvo que exista una sospecha razonable de que hubiese habido algún tipo de posible manipulación” (STS nº 115/2014, de 25 de febrero).

Señala la STS nº 587/2014, de 18 de julio, que la cadena de custodia “…no es prueba en sí misma. La infracción de la cadena de custodia afecta a lo que se denomina verosimilitud de la prueba pericial y, en consecuencia, a su legitimidad y validez para servir de prueba de cargo en el proceso penal”. Ahora bien, ello no supone vulneración de derecho fundamental alguno con el efecto connatural de la nulidad de la prueba refleja, habiendo proclamado la STS nº 656/2015, de 10 de noviembre, que “la irregularidad de la "cadena de custodia" no constituye de por sí, vulneración de derecho fundamental alguno que, en todo caso, vendrá dado por el hecho de admitir y dar valor a una prueba que se haya producido sin respetar las garantías esenciales del procedimiento, y especialmente, el derecho de defensa”.

En definitiva, en todos los casos de registro de dispositivos de almacenamiento masivo de información será necesario que el Juez recoja en la resolución habilitante las concretas garantías que aseguren la integridad y preservación de los datos, garantías que, de ordinario, se proyectarán sobre la recogida de los dispositivos y su posterior conservación.

3.4.4. Incautación de los soportes físicos que contienen los datos

El apartado segundo del art. 588 sexies c contiene una previsión encaminada a evitar al afectado por el registro perjuicios innecesarios que pudieran derivarse de la incautación de los dispositivos. Efectivamente, el papel fundamental que hoy en día desempeñan los dispositivos informáticos en numerosas actividades de la vida cotidiana se traduce en el padecimiento de graves inconvenientes -si no en la imposibilidad- para el desarrollo de esas actividades, en el caso de que los dispositivos sean incautados. Piénsese, por ejemplo, en los ordenadores de una empresa, en los que puede contenerse la contabilidad de la compañía, la gestión de pedidos, los datos de contacto con los clientes y proveedores, etc. En estos casos, la incautación de los ordenadores para proceder a su registro puede suponer el indeseable efecto de la paralización de la actividad mercantil de la compañía, con las graves consecuencias que de ello pueden derivarse.

El precepto establece, como regla general, que no se incauten los soportes físicos que contengan los datos o archivos informáticos *cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos*. Se establecen, no obstante, dos importantes excepciones: que los soportes *constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen*.

El soporte constituirá el objeto del delito cuando recaiga sobre él la acción del sujeto activo o resulte afectado directamente por el daño causado por la conducta delictiva (delitos de daños informáticos, por ejemplo) o cuando contenga los

archivos informáticos de contenido delictivo (delitos de pornografía infantil o contra la propiedad intelectual, por ejemplo). Será frecuente en estos casos que los soportes pertenezcan a la víctima del delito, por lo que deberán intensificarse los esfuerzos para evitarle cualquier perjuicio adicional, siendo en todo caso aplicables las previsiones contenidas en el último párrafo del art. 334 LECrim.

Por el contrario, los soportes físicos podrán ser considerados instrumentos del delito cuando hayan sido directamente utilizados como medio para su perpetración; será el caso, por ejemplo, de los ordenadores utilizados para cometer estafas a través de internet o el teléfono móvil empleado para realizar grabaciones que supongan intromisiones ilícitas en la intimidad. En estos casos, además, procederá siempre su incautación como medida indispensable para llevar a cabo el decomiso que prevén los arts. 127 y siguientes CP.

La existencia de *otras razones que lo justifiquen* aparece como una cláusula genérica de cierre que permitiría valorar como excepción a la regla general cualquier otra circunstancia específica que pudiera darse en un caso concreto, como, por ejemplo, que los soportes físicos contengan datos o archivos informáticos que pertenecieran a un tercero o que el titular o propietario del soporte no tuviera derecho a conservar.

En la determinación de estas razones deberá ponderarse siempre la importancia de las mismas en relación con el perjuicio que genera la incautación del dispositivo.

En estos casos y, sobre todo, cuando la incautación no genere un perjuicio grave a su titular o propietario o no resulte posible obtener una copia en condiciones que garanticen la autenticidad de los datos, los soportes físicos serán siempre incautados. En particular, la imposibilidad de obtener copias en las condiciones que señala el precepto se dará en los casos en los que resulte necesario llevar a cabo un clonado de los dispositivos de almacenamiento y, en atención a la gran cantidad de datos existentes y lentitud del procedimiento, no pueda aquel realizarse durante el desarrollo de la diligencia de entrada y registro. Lógicamente, cuando esto

ocurra, la incautación durará el tiempo mínimo imprescindible para llevar a cabo el volcado de los datos.

Por lo tanto, a la vista de la regulación legal, puede concluirse que las excepciones previstas resultan tan amplias que ofrecerán justificación para incautar los dispositivos en la gran mayoría de los casos. Ello, no obstante, en la medida en que resulte posible, se procurará evitar que de la instrucción penal se deriven perjuicios innecesarios para los afectados por la medida de investigación, adoptando todas las cautelas que resulten necesarias. Así, por ejemplo, en los casos en los que proceda la incautación de los soportes informáticos, no deberá existir inconveniente para facilitar al afectado copias de aquellos archivos existentes en los mismos que no guarden relación con el delito y cuya entrega no perjudique su investigación, siempre que el afectado justifique la necesidad de disponer de los mismos.

3.5. Registro de repositorios telemáticos de datos y ampliación del registro a otros sistemas

Como ya se ha señalado, el registro que regula el art. 588 sexies a incluye también el acceso a repositorios telemáticos de datos. Por otro lado, el apartado tercero del art. 588 sexies c, transcribiendo casi literalmente el contenido del art. 19.2 del Convenio sobre la Ciberdelincuencia, prevé la posibilidad de ampliar los registros judicialmente autorizados a otros sistemas informáticos que sean accesibles desde el que se está registrando. Ambos supuestos presentan ciertas peculiaridades que no concurren en los casos ordinarios de registro de dispositivos de almacenamiento masivo de información, lo que obliga a su análisis conjunto.

Como ya se ha indicado *ut supra*, los repositorios telemáticos de datos son dispositivos de almacenamiento masivo de información a los que se tiene acceso de manera telemática. Pueden formar parte del propio sistema informático del usuario o estar ubicados en sistemas informáticos independientes a los que el usuario accede a través de internet con la finalidad de gestionar la información

digital que allí se encuentra almacenada. Los sistemas pueden ser propios del usuario o ajenos, igual que la información que se almacena en los mismos, que también puede ser propia o ajena, en los casos en los que el acceso a la misma y su gestión forman parte de una actividad laboral, por ejemplo.

Este acceso a información digital de manera telemática constituye la esencia de lo que hoy en día se denomina *cloud computing* (computación en la nube), nuevo concepto que ofrece nuevas respuestas a las demandas que la informática moderna ha venido planteando en los últimos años. La esencia del *cloud computing* reside en sustituir los dispositivos de almacenamiento masivo de información clásicos por el almacenamiento en servidores de internet. Así, la información y, en muchos casos, los programas informáticos, ya no se guardan en el disco duro del ordenador, sino en los servidores a los que se accede a través de internet. Este sistema ofrece la ventaja de proporcionar al usuario capacidades de almacenamiento mucho mayores que las que va a encontrar en su propio dispositivo (ordenador, teléfono móvil, etc.), seguridad en la conservación de sus datos (en muchos casos, estos repositorios se utilizan para hacer copias de seguridad de los datos alojados en el propio sistema informático) y, sobre todo, la posibilidad de acceder a sus datos en cualquier lugar en que se halle desde cualquier dispositivo que se conecte a internet y no solo a través del propio dispositivo en el que tuviera almacenados los datos. Esta posibilidad se revela especialmente útil en el mundo actual de los *smartphones* o teléfonos inteligentes que, por un lado, carecen de capacidad para almacenar grandes cantidades de datos y, por otro, permiten el acceso a los repositorios con una gran movilidad espacio-temporal.

El *cloud computing*, sin embargo, no es el único servicio que permite el almacenamiento de datos a través de internet. Habría que incluir también aquí, por ejemplo, numerosos servicios comerciales que se ofrecen a través de internet, como la banca electrónica, que permite al usuario acceder a su banco y realizar operaciones bancarias, generando con ello información en forma de asientos contables de movimientos, que quedarán almacenados en los servidores de la

entidad bancaria. Igualmente habría que incluir numerosas modalidades de teletrabajo en las que el usuario accede telemáticamente a los sistemas informáticos de la empresa para la que trabaja, gestionando a través de ese acceso diversas formas de información. Finalmente, y aunque podría considerarse también como una forma de *cloud computing*, destacarían algunas herramientas de comunicación, como el correo electrónico, alojado en servidores web a los que el usuario accede telemáticamente. En todos estos casos, aunque no se trata de servicios específicamente destinados al almacenamiento de datos personales, se generan depósitos de información en alojamientos externos a los que se accede a través del dispositivo o sistema propio del usuario.

Pues bien, estas nuevas formas de creación, acceso y gestión de información a través de internet son las que contempla el legislador en los preceptos a los que se ha hecho referencia, previendo la posibilidad de su registro ante la probabilidad de que puedan albergar datos relevantes para la investigación de los delitos. Esa posibilidad debe aparecer suficientemente fundada y motivada, bien desde un primer momento, lo que provocará que el Juez autorice su registro ya en la resolución inicial que dicte (art. 588 sexies a.1), bien como consecuencia de los datos que se obtengan con el registro ya autorizado (por ejemplo, un acceso directo a un repositorio de datos externo), lo que dará lugar a la ampliación del registro que regula el art. 588 sexies c.3.

La primera duda que surge ante la posibilidad de estos registros es la de si los mismos pueden alcanzar únicamente a los repositorios de datos propios del investigado o pueden también extenderse a sistemas informáticos ajenos a los que el investigado acceda a través de su propio sistema, como serían, por ejemplo, su cuenta corriente bancaria o su actividad laboral telemática. Planteada la duda en otros términos, cabría preguntarse si puede accederse a estos datos como parte del registro autorizado o, por el contrario, ello no es posible y es necesario que el Juez se los requiera a la entidad bancaria o empresa en la que trabaje el investigado.

La respuesta positiva parece recogerla el art. 588 sexies c.3, cuando permite el acceso a otro sistema informático, sin especificar la titularidad propia o ajena del mismo, eso sí, condicionándolo siempre a *que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este*. La licitud del acceso, junto con la autorización judicial, se configuran así como los requisitos esenciales para la validez del registro.

El acceso resultará lícito siempre que no derive de alguna diligencia de investigación que vulnere derechos fundamentales como sería, por ejemplo, la obtención de las claves de acceso mediante procedimientos fraudulentos. Resultará, sin embargo, lícito, cuando sean reveladas voluntariamente por el investigado (tal es el caso que resuelve la STS nº 97/2015, de 24 de febrero), o cuando su averiguación derive de la investigación policial previa al registro, o cuando las claves se hayan obtenido con motivo del registro lícito de los dispositivos del investigado, por ejemplo. En cualquier caso, debe tratarse de repositorios o sistemas informáticos a los que pueda accederse desde el sistema inicial para el que se autorizó el registro.

En cuanto a la autorización judicial, es posible distinguir tres supuestos. Que se autorice ya desde el primer momento el acceso a un repositorio telemático de datos o sistema informático externo específicos cuyo uso por el investigado sea conocido; que se autorice de manera genérica el acceso a cualquier repositorio o sistema informático a los que el investigado pueda acceder desde su equipo de manera telemática; o que no se haya previsto este acceso telemático, en cuyo caso establece el precepto la necesidad de recabar autorización judicial ampliatoria, suspendiendo para ello necesariamente la práctica del registro, sin perjuicio de la posibilidad de que la Policía Judicial o el Fiscal, cuando se esté ante un caso de urgencia, puedan llevarlo a cabo. Para este último supuesto establece el precepto la posibilidad de que la Policía Judicial o el Fiscal puedan *llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará*

tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

Esta posibilidad resultará de aplicación ante situaciones de peligro inminente de que la información pueda desaparecer ya que, al resultar accesible a través de internet para cualquier persona que conozca las claves de acceso, podría ser borrada por cualquier tercero que tuviera conocimiento de la detención del investigado, por ejemplo. La circunstancia de que los datos contenidos en sistemas informáticos externos puedan contener información que afecte al derecho al secreto de las comunicaciones (por ejemplo, los correos electrónicos, como se ha dicho), no debe ser obstáculo para admitir su acceso por la Policía Judicial o el Ministerio Fiscal con la convalidación judicial posterior, ya que el art. 18.3 CE exige resolución judicial, pero no impide que esta sea posterior o convalidante. En particular, la regulación contenida en los artículos que se analizan, con la necesaria concurrencia de la nota de urgencia, es suficiente para culminar las exigencias de previsibilidad de la Ley.

El acceso a sistemas informáticos externos puede plantear también problemas de jurisdicción. Efectivamente, la inexistencia de fronteras en internet, unida a los menores costes que para el servicio se generan en determinados países, hará que resulte frecuente que los servidores de almacenamiento de datos estén ubicados físicamente fuera del territorio en el que el Juez que autorice el registro ejerza su jurisdicción (o incluso se desconozca el lugar en que se encuentren localizados). En estos casos, si se parte de una concepción tradicional de los límites de la jurisdicción basada en criterios territoriales, podría parecer más correcto para la obtención de esos datos acudir a mecanismos de cooperación judicial internacional que, sin embargo, resultarían absolutamente incompatibles con la celeridad que requieren este tipo de investigaciones.

Además, en muchos supuestos, o bien se desconoce la localización de los datos (deslocalización) o bien estos se encuentran fragmentados en servidores ubicados en diversos territorios o su ubicación en uno u otro lugar es ajena a la voluntad del

titular de los mismos y depende exclusivamente de la conveniencia técnica u operativa del proveedor de servicios de almacenamiento que modifica la ubicación según sus propias necesidades. Por ello, condicionar la obtención de los datos al lugar donde los mismos se encuentran, conduciría al fracaso de muchas investigaciones simplemente porque se desconoce el lugar exacto de su ubicación, de tal forma que resultarían ineficaces las medidas de cooperación internacional adoptadas.

Ante esta perspectiva, el legislador español se ha decantado decididamente por la licitud del acceso con la simple autorización judicial, incluso en los casos en que los datos se hallen fuera de España. Así se evidencia de la interpretación literal de la regulación legal, y más si se compara con el precedente inmediato, el art. 350.4 de la Propuesta de Código Procesal Penal, que limitaba el acceso a los datos almacenados en sistemas informáticos ubicados en territorio español, remitiendo a la cooperación judicial internacional en el resto de los casos. Esta previsión seguía los criterios del art. 19.2 del Convenio sobre la Ciberdelincuencia que, en su Informe Explicativo, señalaba expresamente que la norma no permitía el registro de sistemas ubicados fuera de las fronteras nacionales propias, remitiendo también a la cooperación judicial internacional para estos casos.

El planteamiento que ahora se realiza, sin embargo, es el de considerar los repositorios telemáticos de almacenamiento como una parte más del sistema que se registra. Lo realmente determinante no va a ser dónde se encuentren físicamente los datos, sino desde dónde se acceda a ellos.

De esta forma, igual que puede afirmarse que el titular de esos datos los posee desde España y ejercita sus derechos sobre ellos desde España y conforme al derecho español, puede afirmarse que cuando se accede a ellos en un registro judicial, se hace en España y conforme al derecho español siempre, claro está, que, como se ha señalado, pueda hablarse de un acceso lícito. De igual modo que resultaría ilógico considerar que el poseedor de pornografía infantil no puede ser perseguido en España si los archivos se encuentran en servidores ubicados en el

extranjero, resultará ilógico considerar que el Juez español no puede acceder a datos de un sistema informático ubicado en España por la circunstancia de que el concreto dato al que se accede se encuentre en un servidor ubicado en el extranjero.

Finalmente, es preciso referirse a la necesidad de adoptar determinadas garantías o cautelas para asegurar la identidad e integridad de la prueba que pueda resultar de los datos almacenados en repositorios o sistemas informáticos externos. Como se ha dicho, las posibilidades de alterar estos datos resultan realmente sencillas, si se tiene en cuenta que el acceso a los mismos dependerá únicamente del conocimiento de las claves. Precisamente por ello, resultará necesaria la adopción de medidas que, o bien impidan la modificación de los datos almacenados, o bien constaten la existencia de determinados datos en un momento temporal preciso.

Entre las primeras destaca el cambio de las claves de acceso por el Juez, evitando de este modo que cualquier persona pueda acceder posteriormente a los datos y los modifique. La decisión de cambiar las claves ha de partir del Juez, al ser éste el competente para la adopción de medidas de conservación de pruebas (art. 326 LECrim), debiendo guardarse las nuevas claves con la debida reserva a fin de que la medida cumpla su cometido. Para ello, bastará con mantener el secreto parcial (en lo que afecte al conocimiento de las claves) de la pieza separada que se forme con la diligencia de registro de los dispositivos de almacenamiento masivo de información (art. 588 bis d). Se cumple con ello la previsión contenida en el art. 588 sexies c.1 cuando señala que el Juez “Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial”.

La segunda forma de garantizar la identidad e integridad de la prueba en estos casos consistirá en asegurar la información que exista en el repositorio o sistema externo en un momento determinado, permitiendo después la utilización del servicio sin ninguna limitación. Para ello, lo ideal será realizar un volcado de la información bajo la fe del Letrado de la Administración de Justicia que, de esta

forma, garantizará el origen y contenido de los datos. Los volcados realizados por la Policía Judicial, en caso de imposibilidad de hacerse por el Letrado de la Administración de Justicia, no gozarán de las garantías que les confiere la intervención de este último, pero podrán hacerse valer como prueba en el juicio oral acompañada de la declaración de los agentes policiales que llevaron a cabo el volcado.

3.6. Registro policial de dispositivos

El art. 588 sexies c.4 ha dado entrada en la regulación de la LECrim a un supuesto que ya venía siendo contemplado desde hacía largo tiempo por la doctrina jurisprudencial. Se trata de la posibilidad de que la Policía Judicial pueda registrar dispositivos de almacenamiento masivo de información sin previa habilitación judicial en los casos de urgencia en los que, además, se aprecie un interés constitucional legítimo que haga imprescindible la medida y, siempre, con convalidación posterior del Juez.

Dispone el precepto que “en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida”.

Como ya se ha venido señalando, con anterioridad a la reforma procesal la jurisprudencia había venido distinguiendo, con motivo del registro de los teléfonos móviles, entre el acceso a la agenda de contactos y el acceso a los datos de comunicación; en el primer caso se entendía afectado el derecho a la intimidad

personal, a diferencia de lo que ocurría en el segundo, que suponía una afectación del derecho fundamental al secreto de las comunicaciones. La consecuencia inmediata que derivaba de este planteamiento era la posibilidad de que la Policía Judicial, en determinados supuestos y con ciertos requisitos, pudiera practicar, sin autorización judicial previa, registros en los teléfonos móviles que no afectaran más que a datos amparados por el derecho a la intimidad y no por el secreto de las comunicaciones (entre otras, STC nº 70/2002, de 3 de abril y 115/2013, de 9 de mayo y SSTS nº 449/2006, de 17 de abril, 1315/2009, de 18 de diciembre y 444/2014, de 9 de junio).

Ahora bien, esta doctrina no significaba que el acceso a los datos íntimos de un teléfono móvil quedara sustraído, como regla general, de la autorización judicial, sino que, por el contrario, únicamente se admitía esta actuación policial cuando se constataran dos importantes requisitos: necesidad de una actuación policial urgente para evitar o averiguar el delito u obtener pruebas incriminatorias y proporcionalidad de la actuación (STC nº 70/2002, de 3 de abril). De esta manera, señalaba la STC nº 206/2007, de 24 de septiembre, que “la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad”.

El fundamento y la esencia de esta doctrina ha sido ahora incorporado a la LECrim, si bien, con dos importantes matizaciones. Por un lado, a diferencia de lo que ocurría en la situación anterior, en la que los registros policiales llevados a cabo en casos de urgencia no requerían ulterior convalidación judicial específica, ahora sí es precisa una resolución judicial posterior al registro policial dictada en un plazo máximo de 72 horas que legitime la injerencia policial en la intimidad. Esta necesidad de convalidación deriva, precisamente, de la segunda de las diferencias que presenta la actual regulación respecto de la situación precedente: con la nueva regulación resultará posible el acceso policial sin previa habilitación judicial a datos

que afecten, no solo al derecho a la intimidad, sino también al derecho fundamental al secreto de las comunicaciones, cuando se den los requisitos de urgencia y necesidad que establece el precepto, cumpliéndose la exigencia constitucional de intervención judicial inmediatamente después del registro. Como ya se ha dicho, la reserva judicial que para este derecho fundamental establece el art. 18.3 CE no exige resolución judicial previa, sino simplemente resolución judicial que, por ese motivo, puede ser posterior o convalidante. En consecuencia, el legislador, consciente de que en el registro de un dispositivo de almacenamiento masivo de información, como puede ser un teléfono inteligente o un ordenador personal, se encontrarán de ordinario datos afectantes al secreto de las comunicaciones, ha permitido su registro policial en supuestos excepcionales, condicionando, eso sí, su validez, a la necesaria convalidación judicial.

Efectivamente, como se señalaba *ut supra*, en la nueva regulación introducida por la reforma procesal, se ha pasado de considerar individualmente los derechos fundamentales que pueden resultar afectados por el registro de un dispositivo de almacenamiento, a contemplar ahora lo que se ha denominado el derecho al entorno virtual de la persona, que supone una nueva realidad que demanda un tratamiento unitario (vid. STS nº 204/2016, de 10 de marzo).

La LECrim condiciona la validez del registro policial previo a la concurrencia de cuatro requisitos: urgencia, interés constitucional legítimo que haga imprescindible la medida, comunicación posterior al Juez en la forma y plazos que se establecen y convalidación judicial de la medida.

La urgencia que exige el precepto no debe interpretarse como urgencia vital para evitar resultados que comprometan intereses especialmente relevantes. Así cabe interpretarlo de la redacción definitiva del precepto en contraste con la contenida en el Anteproyecto, que hablaba en su art. 588 quinquies c de “casos de emergencia o de riesgo de catástrofe o cuando la medida tenga por objeto la localización de personas en situación de urgencia vital”. Ya el informe del Consejo Fiscal a ese Anteproyecto ponía de manifiesto cómo la doctrina jurisprudencial solo venía

exigiendo urgencia e interés constitucionalmente legítimo para el registro policial, habiendo sido esta la postura finalmente acogida por el legislador.

A la urgencia que justifica la intromisión policial en la intimidad sin previa autorización judicial se refiere la STC nº 70/2002, de 3 de abril, como la que resulta necesaria *para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias*. Resultará, por lo tanto, siempre necesario que, de dilatarse el registro policial, se pudiera derivar algún perjuicio para estos fines (así, por ejemplo, la STC nº 115/2013, de 9 de mayo, entendió que la intervención resultó urgente por la necesidad de *averiguar la identidad de alguna de las personas que huyeron cuando fueron sorprendidas, in fraganti, custodiando un importante alijo de droga, evitando así que pudieran sustraerse definitivamente a la acción de la Justicia*).

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 nº 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 nº 133/2016, de 24 de febrero, con cita de la STC nº 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”.

La comunicación al Juez que la Policía Judicial habrá de realizar deberá reunir dos requisitos, uno temporal y otro formal. El requisito temporal determina que la comunicación haya de practicarse en un plazo máximo de veinticuatro horas. Será preciso, por lo tanto, levantar un acta del registro en la que se haga constar, además de otros extremos, la fecha y hora exacta en la que se haya llevado a cabo el registro policial. El plazo legal se contará desde la hora en que tiene lugar el registro hasta la hora de presentación en el juzgado, que se constatará formalmente mediante una diligencia de constancia o acta que se levante al efecto. Como requisitos formales exige la Ley que la comunicación policial se haga al Juez competente mediante un escrito en el que se dé cuenta de las *razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado*. Dentro de estas razones habrá de reflejar la Policía Judicial los motivos de urgencia que impulsaron su actuación, así como el interés constitucionalmente legítimo que la hizo imprescindible; estos serán los motivos que posteriormente deberá recoger el Juez, si los comparte, en la resolución convalidante. Igualmente, deberá reflejarse la actuación realizada, esto es, el concreto registro efectuado, la forma en la que se ha hecho y el resultado obtenido.

El precepto no impide que el Juez pueda requerir de la Policía un nuevo informe ampliatorio del anterior cuando el presentado no colme las exigencias previstas. La indicación de la concreta actuación realizada y la forma de efectuarla servirán también para que el Juez pueda llevar a cabo la ponderación de los intereses en conflicto, valorando la necesidad y proporcionalidad de la medida.

Por último, la resolución judicial que convalide o revoque la medida deberá dictarse en el plazo máximo de 72 horas, contadas, no desde el momento de su notificación policial al Juzgado, sino desde el momento de su realización, de ahí la importancia de consignar el día y hora en que se lleva a cabo el registro, según se ha indicado. La resolución judicial que convalide la medida deberá tener el mismo fundamento que habría tenido de no mediar el registro policial previo, si bien añadiendo al mismo la valoración y ponderación de la pertinencia de la intervención policial previa. Así, tendrá el Juez que justificar la concurrencia de los principios rectores y,

entre ellos, especialmente, la proporcionalidad y necesidad de la medida en el concreto escenario en el que ha sido adoptada, esto es, con carácter previo a la intervención judicial, en atención a la urgencia del caso.

Finalmente, y aunque en el informe policial que justifique la medida ante el Juez deba hacerse constar también el resultado alcanzado con la misma, "la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante, y es susceptible de control judicial ex post, al igual que el respeto del principio de proporcionalidad" (STC nº 70/2002, de 3 de abril, seguida por otras muchas, como las SSTS nº 97/2015, de 24 de febrero y 864/2015, de 10 de diciembre). De ahí deriva que, aunque la medida no arroje resultados relevantes para la investigación o, aunque los resultados contradigan los presupuestos de urgencia, necesidad o proporcionalidad de la medida, el registro policial anticipado será válido si la valoración *ex ante* se encontraba suficientemente justificada.

Por el contrario, "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 este sentido, la citada STC nº 70/2002, de 3 de abril).

3.7. Deber de colaboración

La regulación de los registros de almacenamiento masivo de información en la LECrim termina con una previsión que establece el deber de colaboración con las autoridades y agentes encargados de la investigación, de quienes conozcan el funcionamiento del sistema informático o las medidas de seguridad que protejan los datos. A este deber de colaboración ya se hace referencia en la Circular 1/2019, al abordar el análisis de las disposiciones comunes a todas las medidas de investigación tecnológica, como una de las menciones que habrá de recoger la resolución judicial habilitante (art. 588 bis c.3.h), así como en la Circular 2/2019 en relación con su alcance en el caso de la interceptación de las comunicaciones

telefónicas y telemáticas (art. 588 ter e) y en la Circular 4/2019 en el caso de los dispositivos técnicos de seguimiento y localización (art. 588 quinquies b.3). En consecuencia, con las salvedades y especialidades que a continuación se indicarán, cabe remitirse a lo allí expuesto.

La previsión legal se encarga de precisar el concreto alcance, en los casos de registros de dispositivos de almacenamiento masivo de información, de la genérica obligación de colaborar con los Jueces que imponen los arts. 118 CE y 17 LOPJ. Su inclusión en la LECrim responde, al mismo tiempo, al compromiso alcanzado con la firma del Convenio de Budapest sobre la Ciberdelincuencia, cuyo art. 19.4, prácticamente transcribe. El informe explicativo del Convenio justifica esta previsión como medida necesaria para identificar y obtener los datos que puedan servir de prueba en el proceso ante dos dificultades concretas que pueden encontrarse las autoridades: la dificultad de localizar los datos en sistemas que contengan un gran volumen de información y la dificultad de acceder a los datos protegidos por medidas de seguridad. La obligación de colaboración la justifica, además, como un remedio para evitar que la excesiva duración de los registros llevados a cabo por los investigadores pueda perjudicar a los titulares de los sistemas registrados.

El deber de colaboración debe requerirse en el marco de una investigación por delito, como todas las medidas de investigación tecnológica, por lo que no resulta aplicable a cualquier actuación policial. Son acreedores de esa colaboración las autoridades (Juez o Ministerio Fiscal) y los agentes de Policía Judicial que participen en la investigación. La colaboración resultará procedente para llevar a cabo el registro del dispositivo, sin que pueda imponerse limitación alguna en cuanto al contenido o naturaleza de los datos a registrar, siempre dentro de los términos en que se haya acordado judicialmente la práctica de la diligencia. Como se viene señalando, la regulación de la LECrim tiene por objeto la protección del derecho al entorno virtual del investigado, derecho éste integrado por un conjunto de datos heterogéneos que, individualmente considerados, afectarían a diversos derechos fundamentales. La colaboración, por tanto, podrá afectar al registro de cualesquiera de estos datos.

Los sujetos obligados, destinatarios de este deber de colaboración, serán, según el precepto, las personas que conozcan el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos. Para la interpretación del alcance de esta previsión deberán tenerse en cuenta las reflexiones contenidas en el informe explicativo del Convenio del Cibercrimen a las que antes se hacía referencia. De este modo, cualquier persona que pueda conocer dónde se encuentran ubicados dentro de un sistema informático los datos relevantes que son buscados o que pueda proporcionar información para sortear las medidas de seguridad que pudieran existir para protegerlos, quedará afectada por el deber de colaboración. No tienen por qué ser, necesariamente, personas con conocimientos técnicos que pudieran proporcionar información sobre el diseño o comportamiento de los sistemas de seguridad; se puede tratar de simples empleados de una empresa, incluso de los niveles jerárquicos más bajos, que dispongan de la información que se busca, como podrían ser las contraseñas de acceso a los datos o la ubicación de éstos dentro de la estructura del sistema informático registrado.

Podrán ser destinatarios del deber de colaboración, tanto las personas físicas como las personas jurídicas, aunque únicamente las primeras podrían ser criminalmente responsables del delito que la LECrim anuda a su incumplimiento. Por eso, cuando la información necesaria para el registro obre en poder de una persona jurídica, deberá previamente identificarse la persona física que pudiera tener acceso a ella. Cuando se trate de recabar la colaboración de personas que se encuentren en el extranjero, en principio, deberá emplearse el cauce de la cooperación jurídica internacional.

Los problemas de territorialidad y jurisdicción se harán más patentes en los casos de registro de dispositivos o sistemas informáticos accesibles telemáticamente desde España pero que se encuentren en el extranjero (los referidos *ut supra* como *cloud computing* o computación en la nube). Cuando, en estos casos, se encuentre en territorio español alguna persona que pudiera prestar la colaboración que prevé

el precepto, quedará la misma plenamente sujeta a la obligación, con independencia del lugar donde se encuentren los datos.

No debe confundirse este concreto deber de colaboración que resulta del art. 588 sexies c.5 con las obligaciones que impone el art. 2 de la Ley 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico* (en adelante, LSSICE) a los prestadores de servicios de la sociedad de la información establecidos en España. De igual modo, tampoco pueden extenderse las presunciones de establecimiento en España y sujeción al ordenamiento jurídico español que prevé la citada Ley a los obligados por la LECrim. Por un lado, el deber de colaboración que imponen ambas normas es diferente, pero, además, las consecuencias y sanciones ante su incumplimiento, también son distintas. De esta manera, podría existir un prestador de servicios que cumpliera todas las obligaciones que le impone la LSSICE y, sin embargo, no pudiera facilitar la colaboración que prevé el art. 588 sexies c.5, al no disponer de la información que se le requiere u obrar ésta en sus servicios centrales ubicados en el extranjero.

La obligación de colaboración no solo alcanzará a las personas que tengan relación directa con el sistema informático que se quiere registrar, sino que podría ir mucho más allá, pudiendo requerirse esa colaboración, por ejemplo, del fabricante del concreto dispositivo que forme parte del sistema informático que se registra. El precepto no establece limitaciones en este sentido y, por lo tanto, si los investigadores consideran que el fabricante puede facilitar información, por ejemplo, que permita vencer los sistemas de seguridad del dispositivo para acceder a los datos que almacena, podrán requerir su colaboración en los términos que establece el precepto. Incluso, podría ser requerido un tercero ajeno al sistema y a la fabricación del dispositivo que, en virtud de cualquier clase de conocimientos especializados (por ejemplo, un investigador científico que hubiera analizado un determinado sistema de seguridad), se encontrara en condiciones de facilitar la información a la que se está haciendo referencia.

Se suscitan dudas, también, acerca del alcance de la obligación de colaboración que establece el precepto. Concretamente, cabría plantearse si dicha colaboración se agota con la simple facilitación de información o, por el contrario, podría exigirse una mayor implicación del requerido que llegara, incluso, a desarrollar algún tipo de actividad o trabajo tendente a facilitar el registro del dispositivo, como podría ser, por ejemplo, el desarrollo de un programa informático que permitiera el acceso al sistema que se quiere registrar. El precepto, en este punto, parece claro; lo único que podrán ordenar las autoridades o agentes encargados de la investigación, será la facilitación de información, pero nada más.

El deber de colaboración que impone aquí la LECrim, sin embargo, está sujeto a ciertos límites. Es posible hablar de una limitación subjetiva, que restringiría los sujetos de los que se puede demandar la colaboración, y una limitación objetiva, que exime del deber cuando la colaboración resulte especialmente gravosa.

En cuanto a la limitación subjetiva, el precepto excluye expresamente del deber de colaborar al propio investigado o encausado, sus parientes más próximos y quienes, conforme a lo previsto en el art. 416.2 LECrim, se vean exentos de la obligación de declarar en virtud del secreto profesional. La dispensa que se otorga al investigado o encausado supone una consecuencia lógica del alcance de su propio derecho de defensa y de la facultad que de él deriva, que le permite no declarar contra sí mismo. La exclusión de los parientes (que el precepto concreta en los que, conforme al art. 416.1 LECrim, están dispensados de la obligación de declarar) tiene el mismo fundamento que el que justifica su dispensa de prestar declaración, evitar “el conflicto que eventualmente pudiera planteársele entre su deber legal de decir la verdad y el vínculo de solidaridad y familiaridad, cuando no afectivo, que le uniera con el acusado” (STS nº 459/2010, de 14 de mayo). Finalmente, la inclusión entre estas exclusiones del secreto profesional tiene su justificación en el art. 24.2 CE, que consagra el secreto profesional como una tutela anticipada, de carácter formal, de otros derechos del investigado, como el derecho de defensa y el derecho a la intimidad personal (ATS de 19 de octubre de 2010). Ahora bien, por lo que al secreto profesional se refiere, el art. 588 sexies c.5 limita

los sujetos dispensados de la obligación a los incluidos en el art. 416.2 LECrim, esto es, los abogados, pero no a otros también afectados por el secreto profesional, como podrían ser los traductores o intérpretes (art. 416.3), los eclesiásticos y ministros de cultos disidentes (art. 417.1) o los funcionarios públicos (art. 417.3), por ejemplo.

La limitación objetiva la concreta el art. 588 sexies c.5 señalando que deberán quedar excluidas del deber de colaboración las órdenes de las que pudiera derivarse *una carga desproporcionada para el afectado*. El legislador ha optado por emplear un concepto indeterminado, como es el de la desproporción, que será preciso interpretar. El precedente inmediato de la previsión legal se encuentra, como ya se ha señalado, en el art. 19.4 del Convenio sobre el Cibercrimen, que utiliza el concepto equivalente de la razonabilidad (obligación de facilitar la *información necesaria, dentro de lo razonable*, señala). El informe explicativo del Convenio cita como ejemplo de irrazonabilidad los casos en los que "la divulgación de la contraseña u otra medida de seguridad pudiera poner en peligro injustificadamente la vida privada de otros usuarios o de otros datos cuya revisión no ha sido autorizada".

Al supuesto de afectación de terceros, como es el que señala el informe explicativo, cabría añadir aquellos otros en los que, por ejemplo, la facilitación de información supusiera desvelar secretos industriales que pudieran perjudicar una actividad empresarial del afectado, como resultaría de facilitar información sobre los sistemas de seguridad de un determinado teléfono o dispositivo informático. Realmente, no cabe establecer apriorísticamente los supuestos que pueden presentarse, sino que deberán valorarse las circunstancias concurrentes en cada caso concreto.

En cualquier caso, el Juez, además de la proporcionalidad de la medida, deberá valorar, conforme a los criterios generales que se establecen en la LECrim, la proporcionalidad de la exigencia de colaboración. De esta forma, habrá de justificar que el sacrificio de los derechos e intereses de la persona afectada no resulte

superior al beneficio que para el interés público y de terceros resulte del cumplimiento de ese deber de colaboración. Así, por ejemplo, en los casos de delitos especialmente graves, en los que esté comprometida la vida de alguna persona o la seguridad pública (como ocurriría en los delitos de terrorismo), deberán ceder, de ordinario, los intereses particulares de la persona requerida. Por el contrario, cuando se trate de delitos de menor importancia o cuando los datos que el registro pueda proporcionar a la investigación no sean especialmente determinantes, deberán valorarse con mayor intensidad los intereses del requerido.

Finalmente, no debe olvidarse que siempre que la colaboración requerida genere algún tipo de gasto o remuneración, procederá su resarcimiento, conforme a lo previsto en el art. 17.1 LOPJ.

4. Registros remotos sobre equipos informáticos

4.1. Regulación legal

El Capítulo IX, del Título VIII, del Libro II LECrim aparece dedicado a los *Registros remotos sobre equipos informáticos*, desarrollando en los arts. 588 septies a a 588 septies c, los presupuestos, el deber de colaboración y la duración de este medio de investigación tecnológico. Como ya se adelantaba *ut supra*, esta modalidad de registro, si bien participa de numerosas similitudes y elementos comunes con el registro de dispositivos de almacenamiento masivo de información, ofrece también destacadas especialidades que justifican su tratamiento independiente.

Efectivamente, el registro remoto sobre equipos informáticos presenta como nota común con el registro de dispositivos de almacenamiento masivo el objeto sobre el que recae -ordenador, dispositivo electrónico, sistema informático o, en definitiva, dispositivo de almacenamiento masivo de datos informáticos-, así como la finalidad de la diligencia, la búsqueda de pruebas, indicios o vestigios de la perpetración del delito en los datos digitales almacenados. Sin embargo, existen dos notas esenciales que concurren en los registros remotos y no en los registros directos,

que distinguen ambos tipos de medidas de investigación tecnológica: la clandestinidad y el carácter dinámico del registro.

Por una parte, mientras que los registros directos se llevan a cabo con el conocimiento del afectado, quien podrá consentir o colaborar con el mismo, el registro remoto se desarrolla a sus espaldas. Esta circunstancia puede tener reflejo, no solo en el posible consentimiento o colaboración del afectado, sino en otros extremos que afectan a la diligencia, como las posibilidades de contradicción, el aseguramiento de la prueba o las técnicas que se aplican para su práctica.

Por otra parte, mientras que los registros directos se practican sobre el contenido estático del dispositivo o sistema, los registros remotos pueden conocer, no solo lo que existe en un dispositivo en un momento determinado, sino también lo que se va añadiendo o borrando del mismo durante el tiempo que dure la medida. El carácter dinámico de esta clase de registros determina que pueda accederse a muchos más datos que con los registros directos; es como si se llevara a cabo un registro diario durante todo el tiempo que dura la medida. Una de las consecuencias más importantes que deriva de esta nota es la mayor afectación del derecho al secreto de las comunicaciones que se produce con los registros remotos. El carácter estático del registro propio de los registros directos podrá determinar que resulten afectadas conversaciones puntuales cuyo proceso de comunicación no haya concluido, como podrían ser los correos electrónicos no leídos, mientras que, en los registros remotos, su carácter dinámico posibilita la interceptación de comunicaciones a tiempo real y su seguimiento durante todo el tiempo que dura la medida. Esta circunstancia determina que sea posible considerar que los registros remotos sobre equipos informáticos se encuentran a medio camino entre el registro de dispositivos de almacenamiento masivo de información y la interceptación de comunicaciones telemáticas.

Por eso, sin perjuicio de que en ambas formas de investigación el derecho fundamental que aparece comprometido será el derecho al entorno virtual de la persona, no cabe duda de que con los registros remotos se produce una

intromisión mucho más intensa en el mismo que con los registros directos, lo que va a tener su reflejo, como a continuación se verá, en las exigencias que establece su regulación. Esta será la razón, igualmente, que determina que en este caso no sea posible el registro policial convalidado posteriormente por el Juez, ni en los casos de urgencia, ni cuando se trate de ampliar el registro a otros sistemas, como ocurría con los registros directos.

A este mayor grado de injerencia se refiere el Preámbulo de la Ley Orgánica 13/2015, que justifica en él las mayores limitaciones que establece la regulación para la utilización de esta medida.

La posibilidad de interceptar comunicaciones telemáticas que brinda la diligencia de registro remoto de equipos informáticos puede hacer que sea ésta la técnica elegida para llevar a cabo esa interceptación. Aunque su puesta en práctica resultará, de ordinario, bastante más compleja que otras formas de interceptación de comunicaciones, puede ofrecer ciertas ventajas en algunos casos, como sería, por ejemplo, el acceso a la información ya desencriptada o antes de que haya sido cifrada. Cuando se acuerde la interceptación de las comunicaciones telemáticas a través de las técnicas que se establecen para el registro remoto de sistemas informáticos, pueden plantearse dudas acerca de cuál sea la regulación legal aplicable, si la correspondiente al registro remoto o la aplicable a la interceptación de comunicaciones telemáticas. La solución tiene que venir dada por el contenido de la medida y no por el medio que se emplee. De esta forma, cuando el Juez autorice únicamente la interceptación de las comunicaciones telemáticas, sin acceso a otros contenidos del sistema o repositorios de datos, deberán observarse las disposiciones previstas para la interceptación de comunicaciones; por el contrario, cuando se autorice el acceso al contenido del sistema y el registro de los datos que allí se encuentren, la regulación aplicable será la del registro remoto, independientemente de que la misma también permita la interceptación de las comunicaciones.

En el registro remoto de dispositivos se plantean, también, algunos de los

problemas que surgen en el registro directo, como es, por ejemplo, el referido al ejercicio de la jurisdicción en los casos de ubicación de los datos a registrar fuera del territorio nacional. En este caso, sin embargo, las dificultades que se suscitan son mayores, ya que mientras que en el registro directo de dispositivos de almacenamiento existe un evidente vínculo con el territorio donde se ejerce la jurisdicción, constituido por el equipo informático que se registra y a través del cual se accede a los datos ubicados en el extranjero, los registros remotos, por su propia naturaleza, podrían hacerse sobre cualquier dispositivo o sistema, independientemente de su ubicación.

En estos casos, el criterio deberá ser siempre el de exigir un vínculo territorial con España; el Juez podrá autorizar el registro remoto de un sistema informático que se encuentre en España, aunque a través de él se acceda a datos ubicados en el extranjero, pero no autorizar el registro de un sistema localizado en el extranjero, sin acudir para ello a la cooperación judicial internacional. Como señala el informe del Consejo Fiscal al Anteproyecto, “en tanto en cuanto se tiene acceso al material desde España por un imputado situado en nuestro territorio, el mismo se posee en España, y, consiguientemente, las autoridades españolas tendrían jurisdicción para acceder al mismo”.

4.2. Sistemas de acceso

El art. 588 septies a regula la posibilidad de realizar registros remotos de equipos informáticos a través de dos concretas técnicas: la utilización de datos de identificación y códigos, y la instalación de un *software*. Si bien es cierto que se trata de formas lo suficientemente amplias para dar cabida a los sistemas de acceso que hoy en día pueden ser utilizados, el informe del Consejo Fiscal al Anteproyecto acertadamente demandaba una fórmula más abierta que pudiera amparar formas de acceso remoto que en un futuro puedan ser conocidas.

De los sistemas de acceso previstos, la utilización de datos de identificación y códigos aparece como el más factible. Se trata de utilizar las propias contraseñas

del investigado para acceder, no ya a su ordenador o sistema informático, que sería lo que proporcionaría un conocimiento más amplio de su entorno virtual, sino incluso a reductos de privacidad más limitados pero igualmente útiles para la investigación, como su cuenta de correo electrónico o su cuenta de almacenamiento de datos en la nube (Dropbox, Google Drive, etc.) La mayor complicación que presenta este sistema es la propia obtención de las claves y contraseñas, que debería ser el resultado de una buena investigación policial. Igualmente, puede resultar posible, en algunos casos, requerir dichas claves del proveedor de servicios de internet que almacene los datos, obligado por el deber de colaboración que establece la Ley. Una vez obtenidas las claves, el acceso al sistema o dispositivo a registrar no debería plantear mayores dificultades, salvo en los supuestos en los que el propio proveedor de servicios cuente con sistemas de seguridad que alertan al usuario de un acceso sospechoso a sus cuentas. En estos casos, nuevamente, la solución debe pasar por recabar la colaboración del proveedor de servicios.

Los registros remotos realizados mediante la utilización de “programas espía” resultan más complejos. Estos programas pueden ser de la más variada naturaleza (troyanos, *keylogger*, etc.), pero todos ellos tienen en común permitir a los investigadores, de una u otra forma, acceder a los datos almacenados en un sistema o dispositivo ajeno. Presentan el gran inconveniente de la dificultad de su instalación que, no solo deberá vencer las precauciones del investigado para evitar que se instale en su sistema lo que él no quiere que se instale, sino que también deberá luchar con los posibles programas antivirus que pudiera tener instalados. Por el contrario, ofrece indudables ventajas sobre otros medios de investigación, como serían su instalación y uso sin la necesidad de la intermediación de terceros (como podrían ser las compañías proveedoras de servicios de Internet), la alta cantidad de información sobre el sospechoso que son capaces de proporcionar, su eficacia en dispositivos inalámbricos (a diferencia de la intervención de las líneas ADSL, por ejemplo) o la posibilidad de diseñar el programa para que seleccione la información objeto de registro, lo que ahorraría muchas horas de trabajo a los investigadores.

Las dificultades para la instalación de estos programas espía pueden dar lugar, en algunos casos, a la necesidad de que el Juez tenga que autorizar determinadas actuaciones policiales que afecten a otros derechos del investigado. Este sería el caso, por ejemplo, de la entrada en su domicilio para manipular directamente su equipo informático. No hay obstáculo para admitir esta posibilidad, ya prevista para la captación y grabación de comunicaciones orales mediante dispositivos electrónicos (art. 588 quater a.2), debiendo condicionarse, únicamente, a la existencia de una habilitación judicial específica que deberá valorar la proporcionalidad de autorizar esa concreta diligencia en las circunstancias del caso objeto de investigación.

En definitiva, se trata de medidas que presentan una especial dificultad técnica y cuya utilización aparecerá siempre condicionada por la existencia de una previa labor investigadora que facilite, o bien los datos de identificación o claves del investigado, o bien sus posibles vulnerabilidades para infectar sus dispositivos o sistemas informáticos con un programa espía. Por lo tanto, sin perjuicio de que, como todas las medidas de investigación tecnológica, podría ser acordada de oficio por el Juez o a instancia del Ministerio Fiscal, será normalmente la iniciativa policial la que deberá poner de manifiesto la existencia de posibilidades de utilizarla.

4.3. Ámbito de aplicación

La realización de registros remotos sobre equipos informáticos aparece limitada por el art. 588 septies a a la investigación de alguno de los siguientes delitos: delitos cometidos en el seno de organizaciones criminales, terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional y delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

La limitación de esta diligencia de investigación tecnológica, como ya se ha

señalado, viene determinada por la gravedad de la intromisión en los derechos fundamentales del investigado que con ella se alcanza. De esta manera, aunque pudiera parecer desproporcionada la delimitación de los delitos que permiten su utilización en comparación con los que se establecen para la interceptación de comunicaciones, por ejemplo, no debe olvidarse que a través del registro remoto sobre equipos informáticos es posible, no solo interceptar las comunicaciones telemáticas del investigado, sino también acceder a la totalidad de su entorno virtual, con lo que ello conlleva. Ese es el motivo por el que el legislador ha optado por circunscribir esta medida de investigación a determinadas modalidades delictivas especialmente graves.

Junto a ellas se incluye, como en el caso de otras medidas de investigación tecnológica, la posibilidad del recurso a esta medida en el caso de delitos cometidos a través de instrumentos o tecnologías informáticas o servicios de comunicación. Como ya se señaló en la Circular 2/2019 en relación con la previsión de esta misma clase de delitos como presupuesto para la interceptación de comunicaciones, el fundamento de su inclusión se encuentra en la necesidad de facilitar su persecución, ante la posibilidad de que ésta fuera la única forma posible de perseguir el delito, en atención a su ámbito digital de comisión.

El establecimiento de un catálogo de delitos que delimitan el ámbito de aplicación de la medida supone la concreción de exigencias mínimas en el principio de proporcionalidad para la aplicación de esta medida. Quiere esto decir que cualquier comportamiento delictivo que no esté incluido en la previsión legal no alcanzará la gravedad suficiente para justificar el recurso a esta medida. Ahora bien, igual que ocurre con la interceptación de las comunicaciones telefónicas, la investigación de un delito de esta naturaleza, por sí solo, tampoco garantiza la proporcionalidad de la medida. Será necesario que la resolución judicial, después de justificar que la medida se acuerda para la investigación de uno de los delitos incluidos en el precepto, lleve a cabo un juicio de ponderación que valore si resulta proporcionada la concreta intromisión en los derechos fundamentales del investigado que se producirá con la medida en el caso investigado, en relación con la gravedad del

hecho que se investiga.

Este juicio de proporcionalidad puede determinar que el Juez autorice el registro de ciertos datos del investigado pero no de otros o que, a pesar de investigarse alguno de los delitos previstos en la Ley, considere que no reviste una especial gravedad en el caso concreto para justificar el recurso a la medida. Por ello, no pueden establecerse criterios apriorísticos más allá de la exigencia de que se trate de alguno de los delitos que enumera el precepto.

Finalmente, es preciso destacar que la relación de delitos que establece el artículo supone un catálogo cerrado no susceptible de ser ampliado a otros comportamientos delictivos, por muy graves que estos pudieran ser. Frente a la previsión que recogía el Anteproyecto (que la medida *persiga la investigación de un delito de especial gravedad*, señalaba), el legislador ha optado por suprimir cualquier fórmula abierta que permitiera valorar la proporcionalidad de su aplicación en casos especialmente graves.

4.4. Contenido de la resolución judicial

El art. 588 septies a.2 exige un determinado contenido de la resolución judicial habilitante. Deberá precisar el objeto del registro, su alcance, la forma de acceso al sistema -con especificación del *software* utilizado-, los agentes autorizados para la ejecución de la medida, la autorización, en su caso, para realizar copias y conservarlas, así como las medidas de aseguramiento de los datos registrados. Todas estas menciones, como es lógico, se añadirán al contenido propio de cualquier auto que autorice una medida de investigación tecnológica conforme al art. 588 bis c.

En primer lugar, exige el precepto que se especifiquen *los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida,* así como *el alcance de la misma*. En este

punto resultan aplicables todas las precisiones que se hicieron en relación con el registro de dispositivos de almacenamiento masivo de información.

Cuando se trate de un registro remoto, además, dependiendo de la técnica de acceso que se utilice, será posible que el registro recaiga sobre un dispositivo o repositorio de datos concreto, o sobre todo el sistema informático del investigado. No es lo mismo acceder con sus contraseñas a su cuenta de correo electrónico, que instalar un programa espía en su ordenador personal; mientras que en el primer caso se tendrá acceso, únicamente, a su correo electrónico -tanto el almacenado en las distintas carpetas (enviados, recibidos, eliminados, borrador, etc.) como todo el tráfico que se genere mientras dure la media-, en el segundo, se podrá acceder prácticamente a todo el entorno virtual del investigado (correos electrónicos de todas sus cuentas de usuario, datos almacenados en repositorios remotos, datos almacenados en el propio equipo, actividad en internet, etc.)

La aplicación de los principios rectores de la medida deberá justificar, por lo tanto, el acceso a qué concretos dispositivos resultará necesario, idóneo y proporcionado, para la investigación que se esté llevando a cabo. Además, igual que ocurría con el registro de dispositivos de almacenamiento masivo de información, puede resultar necesario acotar, dentro de la autorización para acceder a determinados dispositivos, los concretos datos que podrán ser registrados y los que no. Así, por ejemplo, puede resultar procedente acceder a la carpeta de correos enviados, pero no a la de los correos recibidos, o acceder a la actividad en internet del interesado, pero no a sus datos almacenados o, en definitiva, acceder únicamente a determinado tipos de datos. Por eso, habrá que estar a las circunstancias concurrentes en cada caso para la determinación del alcance del registro, resultando indispensable para la validez de la medida que la resolución judicial habilitante prevea, precise y justifique ese concreto alcance conforme a los principios rectores.

Exige también la LECrim que la resolución judicial precise la concreta técnica de acceso y, en el supuesto de ser utilizado un programa informático para el registro,

la indicación de éste. La finalidad de estas previsiones no es otra que la de garantizar la legalidad de la medida, facilitando al investigado la información necesaria para el ejercicio de su derecho de defensa.

Cuando se utilicen "programas espía", el precepto exige la indicación de éstos, que habrá que entender referida a la denominación que lo identifique o individualice (su nombre técnico o comercial o el tipo de programa y su fabricante). Con el conocimiento de estos datos podrá el investigado comprobar si efectivamente el programa utilizado permite únicamente lo que el Juez haya autorizado o, por el contrario, va más allá, lo que podría generar vicios de la medida por haberse extralimitado en la intromisión judicialmente autorizada. Puede ocurrir, sin embargo, que no se utilice un programa de uso público, sino un programa desarrollado específicamente para su utilización policial con esta finalidad. En estos casos bastará con indicar el tipo de programa que se utilice (troyano, keylogger, etc.) y, en su caso, su alcance potencial o funcionalidades, sin necesidad de facilitar otros datos técnicos específicos. Debe en este punto recordarse el contenido del acuerdo del Consejo de Ministros de 6 de junio de 2014, que otorga, con carácter genérico, la clasificación de secreto, a los efectos de la Ley 9/1968, de 5 de abril, *sobre secretos oficiales,* a la estructura, organización, medios y técnicas operativas utilizados en la lucha contra la delincuencia organizada por las Fuerzas y Cuerpos de Seguridad del Estado, así como sus fuentes y cuantas informaciones o datos puedan revelarlas.

Si se utilizan las contraseñas o códigos del investigado para acceder al sistema bastará con indicar que ha sido ésta la técnica empleada, sin necesidad de desvelar el modo en el que se obtuvieron tales contraseñas o códigos, cuando formen parte de las técnicas de investigación policial y no existan indicios de la ilegalidad de su obtención, salvo resolución judicial en contrario. Si llegaran a suscitarse dudas por el investigado acerca de la legalidad en la obtención de sus contraseñas o códigos, o del funcionamiento de *software* utilizado, será plenamente aplicable la doctrina jurisprudencial relativa a las dudas de legalidad en la forma de obtención policial del número de teléfono intervenido a un investigado, que

entiende que “no es preciso acreditar la forma de obtención del número de teléfono de un sospechoso cuando no hay indicios de ilegitimidad en el proceso de obtención de la información, ya que es exigible a los poderes públicos que justifiquen que la restricción de un derecho fundamental se ha realizado con respeto a las reglas, pero no lo es que demuestren que no lo han hecho” (SSTS nº 207/2012, de 12 de marzo, 795/2014, de 20 de noviembre o 85/2011, de 7 de febrero, entre otras).

La resolución judicial deberá indicar, igualmente, los agentes policiales que hayan sido autorizados para la ejecución de la medida. Se trata de una precaución necesaria para garantizar su control y facilitar la posibilidad de que el investigado pueda ejercitar su derecho de defensa, comprobando mediante el interrogatorio en juicio de tales agentes policiales la legalidad y alcance de la medida.

La autorización judicial para el registro de sistemas informáticos puede limitarse a permitir el simple visionado y conocimiento de los datos o, por el contrario, puede consentir la grabación de los mismos. El precepto que se analiza exige que, en estos casos, la autorización para copiar y, en su caso, conservar las copias, se refleje en la resolución judicial que acuerda la medida. Aunque la realización de copias debe ser el trámite habitual en la práctica de esta diligencia de investigación como medio indispensable para asegurar la prueba, como ya se indicaba en relación con las copias de los dispositivos de almacenamiento masivo de información, su realización supone una intromisión mayor en los derechos del investigado que la simple visualización de los datos, de ahí la necesidad de su autorización por el Juez.

En la realización de copias de los datos que puedan existir en un momento determinado en un sistema o equipo informático deberá promoverse la intervención del Letrado de la Administración de Justicia como medio indispensable para preconstituir la prueba. Se realizará el volcado de los datos en su presencia, levantándose acta en la que se hagan constar todas las circunstancias del mismo (fecha y hora, alcance, contenido, forma, etc.) y se precintará el soporte en el que

se almacenen los datos volcados, para así garantizar su identidad e integridad. En los casos en los que no resulte posible la presencia del Letrado de la Administración de Justicia, el volcado se llevará a cabo por los agentes facultados judicialmente para la ejecución de la medida, quienes también deberán levantar acta lo más precisa posible de su actuación. En este caso, la práctica de la prueba en el acto del juicio oral requerirá la declaración testifical de los agentes para acreditar la identidad e integridad de los datos volcados.

Finalmente, exige el precepto que la resolución judicial refleje las medidas que se adopten para garantizar la preservación de la integridad de los datos, *así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso*. En realidad, se trata de medidas que tienen por objeto finalidades distintas.

Por un lado, el Juez debe adoptar cautelas -que reflejará en el auto- para garantizar que los datos que existían en un momento determinado en el sistema informático registrado se conserven íntegros hasta el momento de su valoración por el Tribunal de enjuiciamiento. Estas medidas no presentan diferencias sustanciales con las que ya se indicaban para garantizar la integridad de los datos en el caso de registro de dispositivos de almacenamiento masivo de información. Podrán incluirse aquí, además de cualesquiera otras que resulten adecuadas y fueran acordadas por el Juez, la realización de copias en la forma indicada o el cambio de las contraseñas de acceso al sistema informático o repositorio, si bien, en este último caso, teniendo en cuenta que el cambio de las contraseñas alertará al investigado de la intromisión de un tercero en su sistema (lo que puede no ser un inconveniente en los casos, por ejemplo, en que se haya procedido ya a practicar la detención del investigado en el momento de cambiar las contraseñas).

Las medidas para hacer inaccesibles o suprimir los datos del sistema informático registrado serán pertinentes en los casos en los que se trate de sistemas informáticos que ofrezcan material delictivo, como podría ser, por ejemplo, pornografía infantil o archivos que infrinjan derechos de propiedad intelectual.

Como regla general, será preferible hacer inaccesibles los datos antes que suprimirlos, garantizando de esta forma la posibilidad de que puedan ser analizados posteriormente ya que, normalmente, se tratará de datos esenciales para la valoración del comportamiento delictivo investigado. Cuando no resulte posible garantizar la inaccesibilidad de los datos y haya de procederse a su supresión, se adoptarán siempre las cautelas necesarias para la conservación de una copia de los mismos.

4.5. Ampliación del registro

En el caso de los registros remotos de sistemas informáticos la LECrim ha previsto también la posibilidad de ampliar el registro a sistemas distintos del que ya se está registrando cuando, como consecuencia de ese registro, se pueda presumir que los datos buscados se encuentran en un sistema informático diferente. Se reproduce de esta forma la previsión que ya se establecía para el registro de dispositivos de almacenamiento masivo de información, si bien, con una importante salvedad: en los casos del registro remoto no será posible, como sí lo era en los registros directos, llevar a cabo la ampliación del registro sin autorización judicial previa.

La razón parece obvia. En el caso de los registros remotos no existe la urgencia que preside la ampliación del registro cuando se trata de un registro directo. Es preciso recordar que esa urgencia derivaba del conocimiento que tiene el investigado y su entorno más próximo de que se están registrando sus equipos o dispositivos informáticos, lo que podría motivar que, el propio investigado si no está privado de libertad o un tercero que tuviera conocimiento del registro, pudiera acceder remotamente al sistema o equipo en el que se encuentren los datos y los borre o haga inaccesibles, frustrando con ello el posible éxito del registro. En el supuesto que ahora se analiza, por el contrario, al desarrollarse la diligencia a espaldas del investigado, no existe ya ese peligro del que deriva la urgencia motivadora del registro policial previo a la autorización judicial. Por eso, ante la existencia de indicios de que los datos pudieran encontrarse en otro equipo o sistema, deberá necesariamente recabarse la autorización judicial previa para su

registro.

Además de la inexistencia de urgencia, en los registros remotos de equipos informáticos, como se ha señalado, la afectación de los derechos fundamentales del investigado es mucho mayor que en los registros directos, lo que motiva también un incremento de las garantías, que pasa, necesariamente, por suprimir esa posibilidad del registro policial previo a la autorización judicial.

Finalmente, debe recordarse que, en los casos en los que se acuerde la ampliación del registro deberá el Juez dictar una nueva resolución habilitante del mismo que estará sujeta a idénticos requisitos que la resolución original que autorizó el registro del sistema principal. No será extraño en estos casos, sin embargo, que esta nueva resolución judicial se construya, en la mayor parte de sus fundamentos, por remisión a la que ya se haya dictado; el único extremo que requerirá una fundamentación nueva e independiente será el relativo a la necesidad de ampliar el registro al nuevo sistema informático, reflejando los indicios que justifiquen que allí podrán encontrarse datos relevantes para la investigación.

4.6. Deber de colaboración

El art. 588 septies b regula un amplio deber de colaboración de terceros en la práctica de la diligencia de investigación que se analiza. Se trata de una colaboración que excede notablemente de la prevista en el art. 588 sexies c.5 para el registro de dispositivos de almacenamiento masivo de información ya que, en los registros remotos, además de reproducirse el mismo deber de colaboración que ya se preveía para los registros directos, se establece otro todavía más amplio dirigido a *los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos*.

Efectivamente, el apartado segundo del art. 588 septies b reproduce casi literalmente el art. 588 sexies c.5. Se incluye aquí, por lo tanto, el mismo deber de colaboración que ya se analizaba con motivo de los registros directos consistente,

exclusivamente, en la obligación de facilitar información. Igualmente se reproducen las mismas excepciones subjetivas que ya se establecían en el art. 588 sexies c.5 (investigado o encausado y su abogado y personas que están dispensadas de la obligación de declarar por razón de parentesco). Resultará de aplicación, por tanto, a los registros remotos, todo lo que se ha señalado para los registros directos.

La regulación de los registros remotos contiene, sin embargo, una omisión respecto de lo que se establece para los registros directos. En el art. 588 septies b.2 no se incluye, a diferencia de lo previsto en el art. 588 sexies c.5, la posibilidad de que el requerido se excuse de la colaboración demandada cuando de ello se le *derive una carga desproporcionada.*

Esta omisión, sin embargo, debe considerarse relativa. Deberá reconocerse la posibilidad de que el requerido se excuse por suponer para él la colaboración una carga desproporcionada en aquellos casos en los que la colaboración suponga para el sujeto requerido infringir deberes legales o derivados del ejercicio legítimo de sus derechos, de un oficio o de un cargo (art. 20.7º CP). El respeto a los derechos fundamentales también aparece recogido en el art. 591 LEC como fundamento de la excusa del deber de colaboración con la Administración de Justicia.

Es cierto que la Ley prevé expresamente excusas al deber de colaborar con los Jueces y Tribunales en supuestos determinados que no suponen menoscabo en el ejercicio de derechos fundamentales (declaraciones testificales o el propio deber de colaboración del art. 588 sexies c.5, por ejemplo) si bien, ello dependerá de la importancia de la colaboración que quiera ver en ella el legislador para cada caso concreto. En el supuesto de los registros remotos, sin embargo, la Ley ha querido limitar las excepciones al deber de colaboración al mínimo imprescindible (así debe entenderse a la vista de que el legislador no tomara en consideración la advertencia sobre la omisión de la excepción que el informe del Consejo de Estado realizó al Anteproyecto).

Pero, además del deber de facilitar información que el art. 588 septies 2 reproduce, el apartado primero de este mismo precepto amplia, a otros sujetos y con otro objeto, ese deber de colaboración, en términos no previstos por el art. 588 sexies c.5 para los registros directos. Se establece la obligación de prestar *la colaboración precisa para la práctica de la medida y el acceso al sistema*, así como *para que los datos e información recogidos puedan ser objeto de examen y visualización*. Como destinatarios de este deber de colaboración se incluye a *los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro* (el art. 588 ter e, se refiere a *los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual*).

A la hora de interpretar este deber de colaboración no puede perderse de vista que los destinatarios del mismo son, o bien las entidades encargadas de facilitar la comunicación entre los sistemas informáticos o bien los responsables últimos de los sistemas informáticos o bases de datos. Por lo tanto, la colaboración que los mismos podrán prestar y a la que habrá que entender circunscrito el deber que establece la Ley, será la que pudiera facilitarse como intermediador en la comunicación entre los sistemas, o como responsable del diseño y seguridad del propio sistema y, en último término, como responsable de la legibilidad de los datos (*que los datos e información recogidos puedan ser objeto de examen y visualización*, dice el precepto).

Esto hará, por ejemplo, que se pueda requerir la colaboración del prestador de telecomunicaciones para que facilite la inoculación de un virus en el sistema del investigado o del responsable de un sistema informático para que pase por alto la alerta de seguridad que pudiera haber detectado como consecuencia de la monitorización de la actividad del investigado.

De ahí que la diferencia entre el deber de colaboración que establece el apartado primero del art. 588 septies b y el que establece el apartado segundo -y, en definitiva, el que se establece para los registros directos- es que, mientras que en este último caso la colaboración se agota en facilitar información (generalmente las claves o contraseñas o la ubicación de la información buscada, según se dijo), en el primero, la colaboración puede requerir comportamientos activos que exijan el desarrollo de trabajos que posibiliten la práctica de la diligencia de investigación. Pudiera parecer injustificada la distinción que se establece para la colaboración que puede exigirse en ambos tipos de registro, bastante más amplia en el caso de los registro remotos; sin embargo, no debe olvidarse el ámbito mucho más restringido que tienen estos, aplicables únicamente a determinados delitos, lo que justifica, nuevamente, tanto una mayor intromisión en los derechos del investigado, como un deber de colaboración más intenso que permita la efectividad de la diligencia a través de cauces más complejos. Además, la mayor dificultad que entrañan los registros remotos exige, también, mayores herramientas que posibiliten su desarrollo.

Finalmente, el art. 588 septies b incluye, en su apartado tercero, la obligación de guardar silencio que se impone a los sujetos requeridos de colaboración, respecto de las actividades que les hayan sido demandadas por las autoridades, previsión ésta que no se incluía en el caso de los registros de dispositivos de almacenamiento masivo de información. El fundamento de este diferente tratamiento hay que buscarlo en la posibilidad que existe de frustrar la diligencia de investigación en los registros remotos si no se guarda la debida cautela y reserva, cosa que no ocurre en los registros directos, en los que los dispositivos a registrar obran ya en poder de las autoridades y sin que exista la posibilidad de que el investigado pueda manipularlos al conocer que está siendo objeto de investigación judicial.

4.7. Duración de la medida

El art. 588 septies c concluye el Capítulo IX, del Título VIII, con una previsión acerca de la duración del registro remoto: “la medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses”.

Nuevamente la LECrim ha querido reflejar con esta limitación la mayor intromisión en el ámbito de los derechos fundamentales del investigado que con esta medida se produce. Sin rebasar los límites máximos que establece el precepto, la fijación concreta del tiempo de duración de la medida vendrá determinada por la valoración conjunta de los principios rectores en el caso concreto. De esta manera, habrá que atender a la necesidad de la medida, la imposibilidad de progresar en la investigación por otros medios y la gravedad de los hechos objeto de investigación, en relación con el preciso alcance que, para el caso concreto, se fije a la medida.

Pueden suscitarse dudas acerca de cuál debe ser el *dies a quo* que se tome en consideración para el cómputo del plazo, si la fecha que conste en la resolución judicial o el día efectivo en el que se inicie el registro remoto del sistema informático. En este punto existen diferencias importantes con la interceptación de comunicaciones, en la que la aplicación efectiva de la medida se produce de manera casi instantánea a su comunicación al operador de telecomunicaciones. En el caso de los registros remotos, como se ha señalado, no basta con que el Juez autorice la medida, sino que, además, en algunos casos, será precisa una actividad policial previa que consiga el acceso al sistema informático del investigado.

Cuando se utilicen datos de identificación o códigos del investigado no deberían existir problemas, ya que debe entenderse que la Policía Judicial sólo solicitará la autorización judicial cuando ya disponga de esos datos, pudiendo realizarse el registro de manera inmediata a su autorización. Los problemas surgen cuando resulte necesaria la instalación de un software en el equipo del investigado. En estos casos, lógicamente, la autorización judicial deberá ser previa a la actuación

policial, no solo porque en algunas ocasiones dicha autorización resultará precisa para la instalación del *software* (como sería el caso, por ejemplo, en que resultara necesario entrar en el domicilio del investigado para ello), sino porque la propia instalación de ese software sería constitutiva de delito si no media la previa autorización judicial (arts. 197 y 198 CP). Teniendo en cuenta las dificultades que puede llegar a plantear la instalación de ese *software*, no sería extraño que la monitorización se hiciera efectiva cuando ya hubiera transcurrido el plazo de autorización previsto en la resolución judicial.

A diferencia de lo que ocurre con las interceptaciones telefónicas y con la utilización de dispositivos o medios técnicos de seguimiento y localización, en los que los arts. 588 ter g y 588 quinquies c establecen expresamente que el plazo se compute *desde la fecha de autorización judicial*, sin embargo, en la regulación de los registros remotos de equipos informáticos la Ley guarda silencio sobre este extremo, lo que podría interpretarse a favor de la licitud de soluciones distintas. La solución negativa, sin embargo, deriva de la doctrina jurisprudencial desarrollada en torno a la interceptación de comunicaciones telefónicas, señalando la STC nº 205/2005, de 18 de julio, que la Constitución solamente permite "que el secreto de las comunicaciones pueda verse lícitamente restringido mediante resolución judicial (art. 18.3 CE), sin que la intervención de terceros pueda alterar el dies a quo determinado por aquélla", indicando, igualmente, que posponer el inicio del cómputo del plazo al día en que la medida se haga realmente efectiva, "compromete la seguridad jurídica y consagra una lesión en el derecho fundamental, que tiene su origen en que sobre el afectado pesa una eventual restricción que, en puridad, no tiene un alcance temporal limitado, ya que todo dependerá del momento inicial en que la intervención tenga lugar".

En consecuencia, los plazos que establece el art. 588 septies c se computarán, tanto en su duración inicial como en la duración total, desde la fecha de la resolución judicial autorizante.

Finalmente y por lo que se refiere a las prórrogas, ante el silencio de la regulación específica de los registros remotos de equipos informáticos, cabe aquí remitirse a lo expuesto con carácter general para todas las medidas de investigación tecnológica en la Circular 1/2019, sin olvidar que el precepto precisa que *la medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses*.

5. Cláusula de vigencia

La presente Circular no afecta a la vigencia de anteriores pronunciamientos de la Fiscalía General del Estado.

6. Conclusiones

1ª El registro de dispositivos y equipos informáticos limita el denominado derecho fundamental al entorno virtual del individuo. Para llevarlo a cabo será necesaria siempre autorización judicial, independientemente de que resulte afectado el derecho al secreto de las comunicaciones o simplemente el derecho a la intimidad del investigado.

2ª La motivación de la resolución judicial que autorice el registro deberá tener en cuenta la multifuncionalidad de los datos que se almacenan en el dispositivo, justificando conforme a los principios rectores el acceso a cada categoría de datos cuyo registro autorice, en función de la mayor o menor gravedad de los hechos investigados. El ámbito tecnológico de comisión del delito deberá ser especialmente considerado para autorizar el registro.

3ª No será necesaria autorización judicial para el registro de dispositivo de almacenamiento masivo de información cuando el afectado preste su consentimiento al mismo. La prestación del consentimiento podrá hacerse de manera expresa o tácita, aunque siempre de forma inequívoca y libre, sin vicios que la condicionen. Cuando el afectado estuviere detenido, solo será válido el

consentimiento otorgado con asistencia letrada.

4ª La práctica de una diligencia de entrada y registro habilita para la aprehensión de dispositivos de almacenamiento masivo de información, pero no para su registro, que requiere una motivación judicial específica independiente de la que justifica la limitación del derecho a la inviolabilidad domiciliaria. Dicha motivación podrá hacerse en la misma o en diferente resolución judicial del auto de entrada y registro.

5ª La resolución judicial habilitante deberá precisar los concretos dispositivos de almacenamiento masivo de información que podrán ser registrados y, dentro de estos, los concretos datos a los que podrá alcanzar el registro, justificando la decisión conforme a los principios de excepcionalidad, necesidad y proporcionalidad.

6ª Como regla general, deberán realizarse copias del contenido de los dispositivos de almacenamiento masivo de información, llevando a cabo el registro y análisis de los datos que contengan sobre las copias y no sobre los originales. La realización de copias deberá ser siempre autorizada previamente por el Juez.

7ª No será necesaria la presencia del Letrado de la Administración de Justicia durante el clonado de dispositivos de almacenamiento, aunque sí es recomendable para garantizar la identidad de los dispositivos y su integridad en el caso de copias lógicas o selectivas.

8ª En todos los casos de registro de dispositivos de almacenamiento masivo de información será necesario que el Juez recoja en la resolución habilitante las concretas garantías que aseguren la integridad y preservación de los datos, garantías que, de ordinario, se proyectarán sobre la recogida de los dispositivos y su posterior conservación.

9ª Como regla general deberá evitarse la incautación de los dispositivos de almacenamiento masivo de información salvo en los supuestos previstos en la Ley y, en cualquier caso, adoptarse siempre las cautelas necesarias tendentes a evitar que de la instrucción penal se deriven perjuicios innecesarios para los afectados por la medida de investigación.

10ª El registro de dispositivos de almacenamiento masivo de información podrá ampliarse a otros sistemas informáticos que sean lícitamente accesibles desde el que se esté registrando con autorización judicial, ya pertenezcan al propio investigado, ya pertenezcan a un tercero en cuyo sistema el investigado almacene datos.

11ª La jurisdicción de los órganos judiciales españoles se extenderá al registro de cualquier sistema informático que se encuentre en territorio español, con independencia de que los datos se hallen almacenados en servidores ubicados fuera del territorio nacional, siempre que fueren lícitamente accesibles desde el sistema registrado.

12ª Cuando el registro alcance a repositorios telemáticos de datos o sistemas informáticos accesibles telemáticamente desde el que sea registrado, se adoptarán las cautelas necesarias para asegurar la integridad e identidad de los datos almacenados, como, por ejemplo, el cambio de las claves de acceso o el volcado de la información existente.

13ª En caso de urgencia y concurriendo un interés constitucional legítimo, podrá la Policía Judicial llevar a cabo el registro de dispositivos de almacenamiento masivo de información sin habilitación judicial previa, pero siempre con su convalidación posterior. Este registro podrá alcanzar a cualquier dato íntimo o relativo al secreto de las comunicaciones que integre el derecho al entorno virtual del afectado.

14ª El registro resultará urgente cuando sea necesario para la prevención y

averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias, y se ajustará a un interés constitucional legítimo cuando persiga la actuación del *ius puniendi* del Estado, la investigación de los delitos y la determinación de hechos relevantes para el proceso penal.

15ª El deber de colaboración con las autoridades y sus agentes para facilitar el registro de dispositivos de almacenamiento masivo de información alcanzará a cualquier persona que conozca el funcionamiento del sistema informático o sus medidas de seguridad, aunque no llegue a tener ninguna relación con el sistema objeto de registro, como podrían ser los fabricantes de los dispositivos registrados o terceros con conocimientos sobre la seguridad del dispositivo o sistema informático.

16ª Únicamente podrán ser destinatarias de la orden de colaboración las personas que se encuentren en territorio español. La colaboración de una persona que se encuentre en el extranjero deberá recabarse a través de los instrumentos de cooperación jurídica internacional.

17ª El deber de colaboración en el registro comprende la facilitación de la información que resulte necesaria para el mismo, pero no el desarrollo de actividades o trabajos tendentes a posibilitar el registro, como sería el desarrollo de programas informáticos específicos para el registro.

18ª Se exceptúan del deber de colaboración los supuestos que supongan una carga desproporcionada para el afectado. Para valorar la proporcionalidad de la colaboración deberá el Juez ponderar que el sacrificio de los derechos e intereses de la persona afectada no resulte superior al beneficio que para el interés público y de terceros resulte del cumplimiento de ese deber de colaboración.

19ª El registro remoto sobre equipos informáticos conlleva una limitación del derecho al entorno virtual del afectado mucho más intenso que el registro de dispositivos de almacenamiento masivo de información, en atención a su carácter dinámico y su desarrollo sin conocimiento del afectado. Esta circunstancia

determina las mayores exigencias que contiene su regulación en relación con los registros directos.

20ª Cuando las técnicas que prevé la Ley para el registro remoto de equipos informáticos sean utilizadas únicamente para la interceptación de comunicaciones telemáticas, sin acceder al resto de los datos que pudieren existir en un sistema informático, serán de aplicación las previsiones de la LECrim establecidas para la interceptación de comunicaciones telemáticas. Por el contrario, serán aplicables las disposiciones previstas para el registro remoto cuando la medida de investigación autorice el acceso a los datos, independientemente de que también se acceda a las comunicaciones telemáticas.

21ª La resolución judicial que acuerde un registro remoto deberá precisar, conforme a los principios rectores de las medidas de investigación tecnológica, el concreto dispositivo o sistema informático y, en su caso, la clase de datos, a los que se extenderá el registro. Igualmente, deberá señalar la técnica de acceso que se utilice y, si se tratara de un programa informático, la indicación de éste. Cuando se utilicen programas específicamente diseñados para su utilización policial deberá indicarse el tipo de programa utilizado, su alcance potencial y sus funcionalidades.

22ª La realización de copias de los datos registrados remotamente deberá ser autorizada por el Juez. Para la obtención de copias se procurará volcar los datos registrados bajo la fe del Letrado de la Administración de Justicia, adoptándose las cautelas oportunas para garantizar la integridad e identidad de los datos volcados.

23ª En los registros remotos de equipos informáticos, la ampliación del registro a otros sistemas en los que hubiera indicios de encontrarse allí los datos requerirá siempre autorización judicial previa, no siendo posible el registro policial con convalidación judicial posterior.

24ª En los registros remotos se establece un deber de colaboración más amplio y que alcanza a más sujetos que el que se establece para los dispositivos de

almacenamiento masivo de información. Este mismo fundamento justifica que, en estos registros, los sujetos obligados no puedan excusarse de su obligación por la desproporción de la carga que para ellos suponga.

25ª Los plazos de duración que se establecen para el registro remoto sobre equipos informáticos se computarán siempre desde la fecha del auto por el que se acuerde la medida y no desde la fecha de efectividad de la misma.

Madrid, 6 de marzo de 2019

LA FISCAL GENERAL DEL ESTADO

María José Segarra Crespo

EXCMOS/AS E ILMOS/AS SRES/AS FISCALES DE SALA, FISCALES SUPERIORES, FISCALES JEFES PROVINCIALES Y DE ÁREA