Marta Moreno Corte
Abogada

EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO EN EL SENO DE LAS AUTORIZACIONES JUDICIALES DE ENTRADA EN EL DOMICILIO

SUMARIO: 1. INTRODUCCIÓN. 2. LOS DERECHOS FUNDAMENTALES AFECTADOS. 3. EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO: LA INSOSLAYABLE INTERVENCION JUDICIAL. 3.1. La reforma de la Ley de Enjuiciamiento Criminal. 3.2. La aplicación analógica de la legislación penal a los registros efectuados por la Administración tributaria. 4. CONCLUSIÓN: LA NECESIDAD DE UNA DOBLE PONDERACIÓN POR EL JUEZ DE LO CONTENCIOSO-ADMINISTRATIVO.

1. INTRODUCCIÓN

La Administración tributaria está legalmente habilitada para «*entrar*» o «*efectuar registros*» en el domicilio constitucionalmente protegido del obligado tributario cuando «*sea necesario*» (art. 113 LGT)[1] o, concretamente, cuando las actuaciones inspectoras «*lo requieran*» (art. 142.2 LGT). En el curso de esas actuaciones, puede examinar los «*archivos informáticos relativos a actividades económicas*» (art. 142.1 LGT) y adoptar medidas cautelares debidamente motivadas tales como «*el precinto, depósito o incautación*» de «*equipos electrónicos de tratamiento de datos que puedan contener la información de que se trate*» (art. 146.1 LGT)[2].

Más allá de esas previsiones legales, no existe en nuestro ordenamiento tributario ninguna regulación sobre el acceso a los dispositivos de almacenamiento de información que puedan encontrarse en el domicilio (ordenadores, discos duros, correos electrónicos, nube, etc.) ni se exige, en consecuencia, una ponderación específica de las injerencias que

[1] Ley 58/2003, de 17 de diciembre, General Tributaria.
[2] El personal inspector está así facultado para «*verificar y analizar los sistemas y equipos informáticos mediante los que se lleve a cabo, total o parcialmente, la gestión de la actividad económica*» [art. 173.5.f) del Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos (RGGIT)].

pudieran producirse, más allá del derecho a la inviolabilidad del domicilio (art. 18.2 CE), en los derechos a la intimidad (art. 18.1 CE), al secreto de las comunicaciones (art. 18.3 CE) y a la protección de datos (art. 18.4 CE). Y no se exige cuando lo cierto es que los registros y medidas cautelares adoptables por la AEAT afectan a equipos informáticos que pueden contener no solamente «*programas, ficheros y archivos informáticos*» que sirvan de soporte para «*llevar y conservar libros de contabilidad y registros*» o a aquellos otros que «*contengan los datos originarios de los que deriven los estados contables y las autoliquidaciones o declaraciones presentadas*» [art. 29.2. d) LGT], sino también a otros tantos datos personales y privados que entran dentro de la esfera más íntima, personal o familiar del obligado tributario.

Al contrario de lo que está sucediendo en el ámbito penal, la incertidumbre legal que envuelve a este tipo de registros en materia tributaria está provocando en la práctica que la autorización judicial de entrada en el domicilio concedida por el juez de lo contencioso-administrativo esté sirviendo para justificar también el acceso y copiado por parte de la AEAT de la información contenida en los dispositivos de almacenamiento de información, sin valoración alguna de las posibles injerencias en los derechos mencionados. Así, por ejemplo, los autos núm. 166/2019, de 1 de octubre, del Juzgado de lo Contencioso-administrativo núm. 15 de Madrid, núm. 407/2017, de 14 de noviembre, del Juzgado de lo Contencioso-administrativo núm. 32 de Madrid, o núm. 112/2019, de 16 de octubre, el Juzgado de lo Contencioso-administrativo núm. 1 de Cartagena, autorizaron junto con la entrada domiciliaria, sin efectuar ningún tipo de ponderación ni incorporar justificación de alguna clase, el «acceso forzado en el sistema, red, equipos y soportes informáticos» y la obtención de copias en «soporte informático o de papel».

No cabe duda de que, dado el estado actual de las tecnologías de la información, las entradas domiciliarias que se realicen en el seno de las actuaciones tributarias ya no pueden limitarse a la aprehensión de «papeles» con contenido económico (libros de contabilidad, facturas, justificantes, etc.). La Administración tributaria ha de poder acceder a los dispositivos informáticos a la búsqueda de la información con relevancia fiscal. No obstante, habida cuenta de que dicho acceso va a incidir necesariamente en otros derechos fundamentales distintos de la protección constitucional del domicilio, se debe hacer mediante una necesaria habilitación legal y al amparo de una autorización

judicial que, previa ponderación de los intereses públicos y privados en juego, legitime la injerencia. A tal fin, el presente trabajo se dirige a analizar, en primer lugar, la distinción entre los derechos afectados por la entrada domiciliaria y por el registro de dispositivos informáticos; en segundo lugar, la regulación de este tipo de registros en la Ley de Enjuiciamiento Criminal y su posible extensión al ámbito tributario; y, en tercer lugar, la necesidad de una adecuada ponderación de los intereses públicos y privados en juego por los jueces de lo contencioso-administrativo como consecuencia de las injerencias provocadas tanto por la entrada en el domicilio como por el registro de los dispositivos hallados en este último.

2. LOS DERECHOS FUNDAMENTALES AFECTADOS

Como se ha dicho, la Administración tributaria está legalmente habilitada para «*entrar*» o «*efectuar registros*» en el domicilio constitucionalmente protegido del obligado tributario cuando «*sea necesario*» (art. 113 LGT). Eso sí, tal y como exige el art. 18.2 CE, «*ninguna entrada o registro podrá hacerse*» en el domicilio «*sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito*»[3]. De este modo, **la inviolabilidad del domicilio** «constituye un auténtico derecho fundamental de la persona» que garantiza su «ámbito de privacidad» dentro «del espacio limitado que la propia persona elige» y que se caracteriza «precisamente por quedar exento o inmune a las invasiones o agresiones exteriores, de otras personas o de la autoridad pública»[4]. En consecuencia, dejando a un lado el caso del delito flagrante, los únicos títulos legitimadores que pueden hacer decaer la garantía de la inviolabilidad del domicilio en el marco de las actuaciones tributarias son «*el consentimiento*»[5] del obligado tributario titular del domicilio o «*la oportuna autorización judicial*»[6] (arts. 113 y 142.2 LGT y 172.3 RGGIT). Y ante la ausencia del primero, la segunda se convierte en la única forma legítima que tiene la Administración tributaria de entrar en el domicilio del obligado

[3] Sobre estos títulos legitimadores de las entradas y registros en el ámbito de las actuaciones inspectoras, vid. ÁLVAREZ MARTÍNEZ, J.: *La inviolabilidad del domicilio ante la inspección de los tributos*, Ed. La Ley, Madrid, 2007, págs. 179 y ss.

[4] Así, el domicilio inviolable «es un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima» (STC 22/1984, de 17 de febrero, FJ 5).

[5] Acerca del consentimiento, vid. MORENO FERNÁNDEZ, J.I.: "Requisitos para la validez del consentimiento prestado a la entrada en el domicilio por la inspección de los tributos con autorización judicial", en *Estudios en homenaje al profesor Antonio Aparicio Pérez*, Universidad de Oviedo, 2019, págs. 227 y ss.

[6] Sobre el contenido de la autorización judicial, vid. BOSCH CHOLBI, J.L.: "La tutela judicial del derecho a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones ante las actuaciones de la Administración tributaria", en *Revista española de Derecho Financiero*, núm. 192, 2021, págs. 66 y ss.

tributario. Eso sí, no constituye «una suerte de automatismo formal»[7] pues el órgano judicial que la concede debe motivar y justificar formal y materialmente «la necesidad, adecuación y proporcionalidad de la medida de entrada, sometiendo a contraste la información facilitada por la Administración» para que «pueda considerarse constitucionalmente legítima la limitación de tan relevante derecho fundamental»[8]. No hay que olvidar que «la autorización judicial, vista desde la perspectiva de quien ha de usarla, o ese mandamiento para quien ha de sufrir la intromisión, consiste en un acto de comprobación donde se ponderan las circunstancias concurrentes y los intereses en conflicto, público y privado, para decidir en definitiva si merece el sacrificio de éste, con la limitación consiguiente del derecho fundamental»[9].

Ahora bien, aunque la ponderación realizada en la autorización judicial pueda servir para avalar la entrada y el registro en el espacio físico protegido por el derecho a la inviolabilidad del domicilio, en modo alguno puede usarse para legitimar el acceso a los dispositivos electrónicos (ordenadores, correos electrónicos, discos duros, nubes, etc.), en los que coexisten «datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y protección de datos»[10]. En efecto, el art. 18 CE garantiza, además del derecho a la inviolabilidad del «*domicilio*» (apartado 2), los derechos «*a la intimidad personal y familiar*» (apartado 1), al «*secreto de las comunicaciones*» (apartado 3) y a la protección de los datos de carácter personal (apartado 4)[11]. Y, según reiterada doctrina constitucional, «a pesar de las múltiples funciones tanto

[7] La concesión de esa autorización está supeditada a que el juez compruebe los siguientes extremos: «(i) que el interesado es titular del domicilio en el que se autoriza la entrada; (ii) que el acto cuya ejecución se pretende tiene cierta apariencia de legalidad *prima facie*; (iii) que la entrada en el domicilio es necesaria para la consecución de aquélla; y (iv) que, en su caso, la medida se lleve a cabo de tal modo que no se produzcan más limitaciones al derecho fundamental que consagra el artículo 18.2 de la Constitución que las estrictamente necesarias para la ejecución del acto» [STS -Sala de lo Contencioso-administrativo- núm. 1231/2020, de 1 de octubre, FD 3 (recurso núm. 2966/2019)].

[8] STS -Sala de lo Contencioso-administrativo- núm. 1231/2020, de 1 de octubre, FFDD 3 y 5 (recurso núm. 2966/2019). En otras palabras, «para otorgar la autorización debe superarse un triple juicio –que ha de efectuar el juez competente–: el de idoneidad de la medida (toda vez que ésta debe ser útil para la actuación inspectora), el de necesidad (esto es, que no exista otra medida sustitutiva más moderada que la intromisión que se pretende) y el de proporcionalidad en sentido estricto (pues han de ponderarse los beneficios de tal medida para el fin perseguido frente al sacrificio de un derecho fundamental)» (FD 3). Véase, también, la STS -Sala de lo Penal- núm. 85/2019, de 19 de febrero, FD 2 (recurso núm. 361/2018).

[9] SSTC 50/1995, de 23 de febrero, FJ 5; 126/1995, de 25 de julio, FJ 3; y 136/2000, de 29 de mayo, FJ 3.

[10] STC 173/2011, de 7 de noviembre, FD 3. Sobre la protección de los datos personales en este tipo de registros, vid. PÉREZ ESTRADA, M.J.: "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", en *Revista Brasileira de Direito Processual Penal*, Vol. 5, núm. 3, 2019, págs. 1297 y ss.

[11] Este derecho se deriva, tal y como ha indicado el Tribunal Constitucional, del art. 18.4 CE, en virtud del cual *«[l]a ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*» (SSTC 96/2012, de 7 de mayo, FJ 6; y 17/2013, de 31 de enero, FJ 2). Para un análisis en profundidad de este derecho fundamental, vid., OLIVARES OLIVARES,

de recopilación y almacenamiento de datos como de comunicación con terceros a través de internet que posee un ordenador personal, el acceso a su contenido podrá afectar bien al derecho a la intimidad personal (art. 18.1 CE), bien al derecho al secreto de las comunicaciones (art. 18.3 CE) en función de si lo que resulta desvelado a terceros son, respectivamente, datos personales o datos relativos a la comunicación»[12].

Pues bien, el **derecho a la intimidad** tiene por objeto «garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona» frente «a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares», de forma que «atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar frente a [su] divulgación» por terceros[13]. Este derecho, como cualquier otro, puede verse sometido a restricciones, aunque el art. 18.1 CE no prevea «expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad», a diferencia de lo que ocurre con los restantes derechos del art. 18 CE[14]. Ahora bien, para que la afectación del ámbito de intimidad constitucionalmente protegido resulte conforme con el art. 18.1 CE es preciso que concurran los siguientes requisitos: que la intromisión persiga un «fin constitucionalmente legítimo»; que esté «prevista en la ley»; que «como regla general se acuerde mediante una resolución judicial motivada, si bien reconociendo que debido a la falta de reserva constitucional a favor del Juez», la ley puede autorizarla, «siempre y cuando se respeten los principios de proporcionalidad y razonabilidad»[15]; y que se respete el «principio de proporcionalidad»[16].

Por su parte, el contenido del **derecho a la protección de datos** «no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo,

---

B.: *La protección de los datos de carácter personal durante su obtención en España*, Ed. Aranzadi, Pamplona, 2017, apartado RB-1.1 y ss.

[12] SSTC 412/2012, de 2 de julio, FJ 3; y 173/2011, de 7 de noviembre, FJ 3.

[13] SSTC 58/2018, de 4 de junio, FJ 5; y 64/2019, de 9 de mayo, FJ 4.

[14] Resulta pertinente recordar que el art. 18.2 (inviolabilidad del domicilio) prevé como títulos legitimadores el «*consentimiento*», la «*resolución judicial*» y el «*flagrante delito*», y, el art. 18.3 (secreto de las comunicaciones), la «*resolución judicial*». En este sentido, vid., las SSTC 98/2000, de 10 de abril, FJ 5; y 156/2001, de 2 de julio, FJ 4.

[15] Conviene apuntar, como ha hecho MORENO FERNÁNDEZ, J.I., que «[l]a exigencia de una autorización judicial previa para la intromisión en la intimidad de las personas no está prevista en la Constitución y, por tanto, no es exigible en el supuesto de las actuaciones de investigación tributaria sobre los datos económicos de los contribuyentes» ("Carácter reservado de los datos con trascendencia tributaria y publicación del listado de deudores", en *Comentarios a la Ley General Tributaria al hilo de su reforma*, Wolters Kluwer/AEDAF, Madrid, 2016, pág. 157).

[16] SSTC 173/2011, de 7 de noviembre, FJ 2; y 43/2014, de 27 de marzo, FJ 2.

cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal»[17]. Este derecho amplía así «la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado»[18].

Finalmente, el **derecho al secreto de las comunicaciones** se configura como una «garantía autónoma» y no «como manifestación o concreción» del derecho a la intimidad. Ello se fundamenta en que la «intimidad» es un «concepto de carácter material, que atiende al ámbito que cada persona reserva para sí o su familia», mientras que en el ámbito de la protección del secreto de las comunicaciones resulta indiferente «el contenido de la comunicación y su pertenencia al ámbito de lo íntimo»[19]. El concepto de «secreto» es, pues, de carácter «formal» porque «se predica de la comunicación sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado»[20].

Son, entonces, esos tres derechos (intimidad, secreto de las comunicaciones y protección de datos), los que podrían verse afectados en los registros de dispositivos de almacenamiento de información. Así lo ha entendido, en primer lugar, el Tribunal Constitucional, para el que no hay duda de que «**el cúmulo de la información que se**

---

[17] STC 292/2000, de 30 de noviembre, FJ 6. Es importante recordar que «*la cesión de datos de carácter personal que se deba efectuar a la Administración tributari*a» no requiere «*el consentimiento del afectado*» (art. 94.5 LGT). Eso sí, «*[l]os datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros*» salvo en los supuestos legalmente establecidos (art. 95.1 LGT). Y, en todo caso, la Administración tributaria debe adoptar «*las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado*» y debe guardar el «*más estricto y completo sigilo respecto de ellos*» (art. 95.3 LGT). Así, por ejemplo, según ha indicado el TSJ de Madrid, si en los ficheros inspeccionados se recogen no solo datos con trascendencia tributaria, sino también historiales clínicos, no habrá conculcación del derecho a la protección de datos si resulta «acreditada la trascendencia tributaria de la información y documentación recabada» y si la inspección incorporó los «detalles de pago», pero blanqueó las copias suprimiendo «los datos médicos» para que no hubiese en el procedimiento «documento alguno donde figure junto al nombre y apellidos del paciente el detalle del tratamiento o intervención» [STSJ de Cataluña -Sala de lo Contencioso-administrativo- de 23 de marzo de 2021, FD 2 (recurso núm. 576/2019)]. Sobre estas cuestiones, vid. HERRERO DE EGAÑA ESPINOSA DE LOS MONTEROS, J.M.: "Intimidad, tributos y protección de datos", en *InDret*, núm. 2, 2007, págs. 14 y ss.

[18] SSTC 151/2014, de 24 de septiembre, FJ 7; y 96/2012, de 7 de mayo, FJ 6.

[19] STC 18/2020, de 10 de febrero, FJ 3.

[20] SSTC 114/1984, de 29 de noviembre, FJ 7; 34/1996, de 11 de marzo, FJ 4; y 170/2013, FJ 4.a).

almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.)» **forma parte «del ámbito de la intimidad constitucionalmente protegido»**, dado que «a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano»[21]. No hay que descuidar que, aun cuando los «datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente», analizados en su conjunto configuran, sin duda, 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»[22].

Así lo ha entendido, en segundo lugar, el Tribunal Supremo para quien «los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores», de modo que su contenido «no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario» porque en ellos coexisten **«datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y protección de datos»**[23].

Por último, también el legislador ha regulado a través de 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 (en adelante, LO 13/2015), «las medidas de investigación tecnológica» que inciden **«en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución»** (apartado I del Preámbulo), entre las que se encuentra el registro de dispositivos informáticos de almacenamiento masivo.

[21] STC 173/2011, de 7 de noviembre, FJ 2.
[22] STC 173/2011, de 7 de noviembre, FD 3. Por ese motivo, «la regulación legal del registro de dispositivos y sistemas informáticos» ha venido siendo demandada «por los Tribunales al resultar evidente la trascendencia que para la tutela de los derechos fundamentales podía suponer la protección del contenido almacenado» (Circular 5/2019, de 6 de marzo, de la fiscal general del Estado, sobre registro de dispositivos y equipos informáticos, pág. 30160).
[23] STS -Sala de lo Penal- núm. 342/2013, de 17 de abril, FD 8 (recurso núm. 1461/2012).

3. LOS REGISTROS DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO: LA INSOSLAYABLE INTERVENCIÓN JUDICIAL

3.1. La reforma de la Ley de Enjuiciamiento Criminal

Hasta el año 2015, la legislación penal se refería exclusivamente a «*la entrada y registro en lugar cerrado, del de libros y papeles y de la detención y apertura de la correspondencia escrita y telegráfica*» (antiguo título VIII LECrim; actuales Capítulo I y II del Título VIII LECrim sobre «*medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*»). No existía, sin embargo, ninguna previsión relativa a los registros de los dispositivos informáticos. Por ello, el Tribunal Constitucional, en un asunto referente al acceso a la información almacenada en un ordenador, apuntó la necesidad de «establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información»[24].

En ese contexto de vacío normativo, como ha indicado la Fiscalía General del Estado, «el modo habitual de proceder era el de considerar amparado [el] registro por la resolución judicial que autorizaba la entrada en el domicilio»[25]. Fueron surgiendo, no obstante, construcciones jurisprudenciales que limitaron ese automatismo en el acceso a los dispositivos informáticos con la sola existencia de una autorización legal para la entrada domiciliaria. En un primer momento, el tratamiento del registro del contenido de este tipo de dispositivos difería en función de si el derecho afectado era el derecho a la intimidad o el derecho al secreto de las comunicaciones[26]. Y ello porque, a diferencia de lo que ocurre con la entrada y registro en el domicilio o en la intervención de comunicaciones, «respecto de las restricciones del derecho a la intimidad» no existe «en la Constitución reserva absoluta de previa resolución judicial»[27]. Es más, «no es constitucionalmente exigible que sea el Juez quien tenga que autorizar esta medida limitativa, pudiéndola adoptar, siempre que una ley expresamente la habilite, la autoridad que, por razón de la materia de que se trate, sea la competente»[28]. La delimitación del

[24] STC 173/2011, de 7 de noviembre, FD 3.
[25] Circular 5/2019, de 6 de marzo, cit., pág. 30168.
[26] Circular 5/2019, de 6 de marzo, cit., pág. 30161.
[27] SSTC 70/2002, de 3 de abril, FJ 3; y 233/2005, de 26 de septiembre, FJ 7.
[28] STC 234/1997, de 18 de diciembre, FJ 9.

contenido de cada uno de estos derechos dependía, además, del «carácter de la información» a la que se accedía[29]. Así, la comunicación telemática en sus distintas modalidades de conversación (oral o escrita) se encontraba afectada por el derecho al secreto de las comunicaciones, mientras que, una vez terminada la comunicación, su conservación y documentación concernía al «derecho a la intimidad y/o, en su caso, a la autodeterminación informativa mediante el control de datos personales»[30].

Más tarde, el Tribunal Supremo abogó por «la necesidad de un tratamiento unitario» a través de «la proclamación de un **derecho del individuo al entorno digital**» como un «derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional»[31]. 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», que 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»[32]. A lo anterior, añadió que «**tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante**»[33]. De este modo, el acceso a la información

[29] STC 142/2012, de 2 de julio, FJ 3.
[30] STS -Sala de lo Penal- núm. 462/2019, de 14 de octubre, FD 1 (recurso núm. 1379/2019). Este tratamiento individualizado cedió, como ha indicado PÉREZ ESTRADA, M.J., «ante el cúmulo de datos contenidos en los dispositivos de almacenamiento que hace que resulte imposible identificar de manera aislada los derechos fundamentales implicados, pues, muchas veces, aparecen entremezclados» [en "La protección de los datos (…)", en *Revista Brasileira de Direito Processual Penal*, Vol. 5, núm. 3, 2019, ob. cit., pág. 1311].
[31] STS -Sala de lo Penal- núm. 462/2019, de 14 de octubre, FD 1 (recurso núm. 1379/2019).
[32] STS -Sala de lo Penal- núm. 342/2013, de 17 de abril, FD 8 (recurso núm. 1461/2012).
[33] STS -Sala de lo Penal- núm. 462/2019, de 14 de octubre, FD 1 (recurso núm. 1379/2019). Para la Fiscalía General del Estado, «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». Ciertamente, «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», de forma que «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» (Circular 5/2019, de 6 de marzo, cit., pág. 30162).

contenida en un equipo informático requerirá «el presupuesto habilitante de una autorización judicial»[34].

Así las cosas, la reforma operada por la LO 13/2015 intentó poner fin al «*vacío normativo*» existente respecto de los «*registros de dispositivos informáticos de almacenamiento masivo*» (apartado IV del Preámbulo de la LO 13/2015). En la línea de la jurisprudencia existente, implantó la necesariedad de una «*motivación individualizada*» por parte del juez cuando «*con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos*» (art. 588 sexies a LO 13/2015). De este modo, la nueva regulación partió «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 que se acceda a su contenido**[35]. Así lo especifica el art. 588 sexies a.2 LO 13/2015, en virtud del cual «*la simple incautación de cualquiera de los dispositivos [de almacenamiento masivo], practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente*». Por lo tanto, en ausencia del consentimiento eficaz del «titular o usuario del equipo informático afectado»[36], el «*juez*» debe justificar «*las razones que legitiman el acceso*» desde el punto de vista de la información contenida en tales dispositivos (art. 588 sexies a LO 13/2015).

El acceso al contenido de la información alojada en un equipo informático requiere entonces «una habilitación judicial específica, distinta de la concedida para una entrada y

[34] STS 342/2013, de 17 de abril, FD 8. Acerca del derecho al propio entorno virtual, vid. FERNÁNDEZ-GALLARDO, A.J.: "Registro de dispositivos de almacenamiento masivo de información", en *Dereito*, Vol. 25, núm. 2, 2016, págs. 33 y ss.; y PÉREZ ESTRADA, M.J.: "La protección de los datos (…)", ob. cit., págs. 1311 y ss.

[35] Circular 5/2019, de 6 de marzo, cit., pág. 30168.

[36] El consentimiento constituye una «fuente de legitimación constitucional» de las injerencias en los derechos fundamentales del art. 18 CE (STC 54/2015, de 16 de marzo, FJ 5). Al igual que ocurre con el derecho a la inviolabilidad del domicilio, el consentimiento eficaz del sujeto «permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno» (SSTC 83/2002, de 22 de abril, FJ 5; y 173/2011, de 7 de noviembre, FJ 2). Eso sí, ha de realizarse por «el titular o usuario del equipo informático afectado y en relación a un asunto concreto del que tenga conocimiento quien lo presta, sin que se pueda aprovechar para otros fines distintos»; prestarse consciente y libremente en condiciones de «serenidad y libertad ambiental» (STS -Sala de lo Penal- núm. 311/2020, de 15 de junio, FD 3); de forma «verbal o por escrito»; y expresa o tácitamente «mediante actos propios, de colaboración o de no oposición que revelen de modo inequívoco la voluntad del sujeto» [STS -Sala de lo Penal- núm. 311/2020, de 15 de junio, FD 3 (recurso núm. 3777/2018)].

registro», bien «en el mismo auto», bien «en resoluciones independientes»[37]. En otras palabras, la autorización para registrar tales dispositivos «no está incluida en la resolución judicial previa para acceder al domicilio en el que […] se encuentran instalados», de manera que «el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías»[38]. Siendo así, la autorización judicial debe fijar «*los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos*» (art. 588 sexies c LECrim).

3.2. La aplicación analógica de la legislación penal a los registros efectuados por la Administración tributaria

El Tribunal Supremo ha recalcado que «el acceso al contenido de la información alojada en un equipo informático requiere una habilitación judicial específica, distinta de la concedida para una entrada y registro». Lo dijo «antes la jurisprudencia y lo dice ahora la Ley de Enjuiciamiento Criminal»[39]. La duda que podría suscitarse es, sin embargo, si tal regulación puede extenderse a los registros de dispositivos llevados a cabo por la Administración tributaria en el marco de las entradas domiciliarias de los obligados tributarios ante el vacío normativo existente al respecto, cuestión esta que ya ha sido planteada ante el Tribunal Superior de Justicia de Madrid a través de un recurso interpuesto contra el citado auto núm. 166/2019, de 1 de octubre de 2019, del Juzgado de lo Contencioso-administrativo núm. 15 de Madrid. En aquel recurso se alegó que, al haber autorizado el juez «el acceso forzado en el sistema, red, equipos y soportes informáticos» con la entrada domiciliaria, este obvió la LO 13/2015 «que tiene rango de ley orgánica y es posterior a la Ley General Tributaria», y que exige una autorización específica para el registro de los dispositivos de almacenamiento masivo. Para el Tribunal Superior de Justicia de Madrid, por el contrario, **la LO 13/2015 no resultaría de aplicación a las entradas y registros previstos en la LGT porque su «ámbito propio y exclusivo es la instrucción de las causas penales»**[40]. La decisión adoptada por el TSJ de Madrid es, sin embargo, objetable por las siguientes razones:

[37] STS -Sala de lo Penal- núm. 311/2020, de 15 de junio, FD 3 (recurso núm. 3777/2018).
[38] STS -Sala de lo Penal- núm. 342/2013, de 17 de abril, FD 8 (recurso núm. 1461/2012).
[39] STS -Sala de lo Penal- núm. 311/2020, de 15 de junio, FD 3 (recurso núm. 3777/2018).
[40] STSJ de Madrid -Sala de lo Contencioso-administrativo- núm. 238/2020, de 24 de junio, FD 3 (recurso núm. 809/2019).

1. El Tribunal Constitucional consideró **«muy razonable»**, hace casi treinta años, **la aplicación «por analogía» del «único precepto legal existente»** (antiguo art. 87.2 LOPJ)[41] a las entradas en el domicilio desarrolladas en la actividad inspectora dadas «las características de tal actuación administrativa, muy cercana en más de uno de sus eventuales aspectos a la jurisdicción penal como consecuencia de la equiparación del injusto de tal naturaleza y del administrativo»[42]. Y, además, «con una concepción idéntica», consideró **«clara» la aplicación «analógica» de los preceptos de la Ley de Enjuiciamiento Criminal** dedicados a «los registros domiciliarios dentro de la fase de instrucción en causas por delito» al procedimiento de la inspección tributaria, el cual «desemboca frecuentemente en un procedimiento sancionador y puede terminar en manos del Fiscal por un eventual delito tributario»[43]. Por la misma razón, puede considerarse «muy razonable» o muy «claro» que se aplique «por analogía» el «único precepto legal existente» (el art. 588 sexies a LECrim) a los «registros de dispositivos de almacenamiento masivo» desarrollados en el marco de las entradas domiciliarias de la Administración tributaria.

2. El Tribunal Supremo ya ha indicado, en el marco de las entradas domiciliarias de la Administración tributaria, que si no se exigiesen al juez las «garantías formales y materiales como requisitos estrictos y excepcionales para sacrificar el contenido esencial» del derecho fundamental a la inviolabilidad del domicilio, el afectado por sus actuaciones **se encontraría «en una situación más desfavorable y gravosa para el disfrute pleno de ese derecho que la que ocupa el encausado en una instrucción penal, para el caso en que se solicite y autorice la entrada en su domicilio**»[44]. Por esta razón, es necesario que las mismas garantías «formales y materiales» que se exigen para los registros de dispositivos de almacenamiento masivo llevados a cabo en el seno de actuaciones desarrolladas en sede penal, se impongan a los efectuados en sede administrativa, pues unos y otros implican un sacrificio del contenido de los derechos a la intimidad, al secreto de las comunicaciones a la protección de datos personales del obligado tributario afectado.

---

[41] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Según el antiguo art. 87.2 LOPJ, correspondía a los juzgados de instrucción autorizar «*en resolución motivada*» las entradas domiciliarias cuando ello procediese para «*la ejecución forzosa*» de los actos de la Administración.
[42] STC 50/1995, de 23 de febrero, FJ 6.
[43] STC 50/1995, de 23 de febrero, FJ 7.
[44] STS -Sala de lo Contencioso-administrativo- núm. 1163/2021, de 23 de septiembre, FD 2 (recurso núm. núm. 2672/2020).

3. La pretensión del legislador con la regulación de los registros de los dispositivos informáticos ha sido precisamente, como ha puesto de manifiesto la Audiencia Provincial de Madrid, tanto **«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»** como exigir al juez que «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»[45]. Resultaría entonces llamativo que, en materia tributaria, sí se permitiese que esa autorización judicial amparase cualquier «acto de injerencia» incluso cuando desbordase el contenido «material» del art. 18.2 CE.

En suma, ni la autorización judicial de entrada en el domicilio (art. 18.2 CE), ni la habilitación legal para adoptar medidas cautelares como «*el precinto, depósito o incautación*» de *«equipos electrónicos de tratamiento de datos que puedan contener la información de que se trate*» adoptables en el procedimiento de inspección (art. 146.1 LGT), pueden fundamentar el acceso automático al contenido de los dispositivos electrónicos, como está ocurriendo en la práctica. A la vista del vacío normativo existente en materia administrativa, y en tanto no haya una intervención legislativa en tal sentido, se impondría como única solución posible la de extender analógicamente los postulados de la LECrim al registro de dispositivos de almacenamiento de datos, cualquiera que sea el ámbito en el que se efectúe. Admitir lo contrario supondría que «en la actualidad el registro que se produce con autorización judicial en el ámbito penal resulta[ría] más restrictivo que el que se lleva cabo por los órganos de inspección, cuando en ambos casos nos referimos a la limitación de derechos fundamentales»[46].

Esa aplicación extensiva de la LECrim a los registros de los dispositivos de almacenamiento masivo desarrollados por la Administración tributaria no significaría, sin embargo, como han sostenido algunos autores, que el juez de instrucción fuese el único competente para otorgar la correspondiente autorización[47]. La aplicación analógica de

[45] SAP de Madrid -Sección 30ª- núm. 353/2020, de 24 de septiembre, FD 3 (recurso núm. 655/2020).
[46] RUIZ HIDALGO, C.: "Reflexiones acerca de la entrada y registro del domicilio constitucionalmente protegido: especial referencia a los dispositivos electrónicos y virtuales", en *Revista española de Derecho Financiero*, núm. 190, 2021 (Aranzadi BIB 2021\3255), pág. 39.
[47] Así, por ejemplo, para RUIZ HIDALGO, C., «el registro propiamente dicho de un dispositivo o un soporte digital que no sea propiedad de la empresa» no «se puede autorizar por un juez de la jurisdicción contencioso-administrativa», dado que «en nuestro ordenamiento sólo se permite el registro de dispositivos

aquella regulación no afectaría, a nuestro entender, a la competencia del juez de lo contencioso-administrativo para prestar dicha autorización. Es el «juez» el que debe erigirse en el «encargado de garantizar la ponderación previa de los derechos e intereses en conflicto y de prevenir eventuales vulneraciones del derecho fundamental» afectado[48]. Y lo es, en cada caso, el del orden jurisdiccional al que corresponda la materia cuyo conocimiento le haya sido atribuido. Por tanto, el hecho de exigir al juez de lo contencioso-administrativo que justifique «*las razones que legitiman el acceso*» de la Administración tributaria a la información contenida en tales dispositivos, en los mismos términos que se le están exigiendo al juez de instrucción, no implicaría la asunción por parte del primero de la valoración de cuestiones que puedan corresponder al segundo. Se trataría únicamente de no ceñir su papel de *juez de garantías* a las entradas domiciliarias, para extenderlo también a aquellas injerencias ocasionadas por el registro[49]. No hay que olvidar, de un lado, que, conforme a la LOPJ, son los jueces y tribunales los que garantizarán los derechos y libertades fundamentales «*bajo la tutela de los mismos*» (art. 7.1). Y, de otro, que, de acuerdo con la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, «*[l]os Juzgados y Tribunales del orden contencioso-administrativo conocerán de las pretensiones que se deduzcan en relación con la actuación de las Administraciones públicas sujeta al Derecho Administrativo*» (art. 1.1)[50].

---

de almacenamiento masivo de información, ya sea de forma remota o presencial, en el caso de que exista una autorización del juez del orden penal» tal y como se regula en el art. 588 sexies LO 13/2015 [“Reflexiones acerca de la entrada y registro (…)”, ob. cit., pág. 37]. Y, según BOSCH CHOLBI, J.L., caben dos opciones: o bien se aplica por analogía la regulación de la LOPJ y LJCA sobre las entradas domiciliarias a los registros de dispositivos de almacenamiento masivo, en cuyo caso el juez competente será el de lo contencioso-administrativo; o bien se aplica por analogía la regulación sobre dispositivos de almacenamiento masivo de la LECrim, en cuyo caso el juez competente será el de instrucción [en “La tutela judicial (…), ob. cit., pág. 62].

[48] STS -Sala de lo Contencioso-administrativo- núm. 1231/2020, de 1 de octubre, FD 3 (recurso núm. 2966/2019).

[49] Efectivamente, tomando las palabras de BOSCH CHOLBI, J.L., «en la medida en que se estima que la entrada domiciliaria no tiene un fin en sí misma, en este ámbito tributario, si no va a acompañada del registro, y que el Juzgado de lo contencioso-administrativo, en unidad de acto, se encuentra en mejor posición para adverar, asimismo, el cumplimiento de los requisitos constitucionales y legales para autorizar la intromisión en el derecho del art. 18.4 CE» no «debe preterirse que la autorización judicial que permita acceder a ese ámbito reservado, lejos de limitarse a una mera coletilla que amplíe sin fin el ámbito administrativo de actuación, debe dejar expresa constancia de todas aquellas garantías dirigidas a proteger ese concreto derecho fundamental –y, especialmente, el específico cumplimiento del principio de proporcionalidad–» [en “La tutela judicial (…)”, ob. cit., pág. 62].

[50] Además, el carácter «universal» de la protección de los derechos fundamentales justifica que sea el mismo juez el que resuelva las autorizaciones sobre las entradas domiciliarias y los registros de dispositivos que afectan a la materia para la cual tiene reconocida la competencia. Una interpretación parecida hizo el legislador, respecto de los juzgados de lo mercantil, en la reforma operada por Ley Orgánica 8/2003, de 9 de julio, para la Reforma Concursal, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (apartado II de la Exposición de Motivos).

4. CONCLUSIÓN: LA NECESIDAD DE UNA DOBLE PONDERACIÓN POR EL JUEZ DE LO CONTENCIOSO-ADMINISTRATIVO

La protección constitucional del registro de dispositivos de almacenamiento masivo que se encuentren en el domicilio constitucionalmente protegido de los obligados tributarios no se limita al derecho a la inviolabilidad del domicilio (art. 18.2 CE), sino que extiende a los derechos a la intimidad (art. 18.1 CE), al secreto de las comunicaciones (art. 18.3 CE) y a la protección de datos (art. 18.4 CE). Así lo han recalcado, primero, los tribunales en una línea jurisprudencial clara y, más tarde, el legislador con la implantación, en la LECrim, de una habilitación judicial específica que pondere la intromisión provocada por tales registros.

La regulación existente en la LECrim debería ser aplicada a los registros de tales dispositivos llevados a cabo por la Administración tributaria en el marco de las actuaciones inspectoras, siendo el juez de lo contencioso-administrativo quien debe realizar una doble ponderación: la de la entrada domiciliaria, de un lado; y la del registro y acceso al contenido de los dispositivos de almacenamiento masivo, de otro. Solo así podría decidir si «las circunstancias concurrentes y los intereses en conflicto» merecen «la limitación consiguiente [de los] derecho[s] fundamental[es]»[51]. En fin, no cabe olvidar que «nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos», de forma que «se hace imprescindible asegurar su protección» frente «a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada»[52].

[51] STC 50/1995, de 23 de febrero, FJ 5.
[52] STC 119/2001, de 24 de mayo, FJ 5.