REGISTRO POR LA ADMINISTRACIÓN TRIBUTARIA DEL CONTENIDO ALMACENADO EN UN ORDENADOR PERSONAL: REQUISITOS QUE DEBEN REUNIR TANTO LA SOLICITUD COMO LA AUTORIZACIÓN JUDICIAL: STS DE 29 DE SEPTIEMBRE DE 2023, REC. NÚM. 4542/2021

Leopoldo Gandarias Cebrián
Abogado y profesor de Derecho Financiero y Tributario
Universidad Complutense de Madrid (España)

Resumen

Entre otras consideraciones relevantes, la doctrina legal sentada por la Sección Segunda de la Sala Tercera del Tribunal Supremo en relación con las exigencias de la autorización de acceso y entrada a domicilios constitucionalmente protegidos es extensible a aquellas actuaciones administrativas que tengan por objeto el acceso y tratamiento de la información almacenada en dispositivos electrónicos (ordenadores, teléfonos móviles, tabletas, memorias, etc.) que pueda resultar protegida por los derechos fundamentales a la intimidad personal y familiar y al secreto de las comunicaciones.

Palabras clave

Registro por la Administración tributaria del contenido almacenado en un dispositivo electrónico.

Abstract

Among other relevant considerations, the doctrine established by the Second Section of the Third Chamber of the Supreme Court, concerning the requirements for authorization to access and enter constitutionally protected domiciles, extends to administrative actions aimed at accessing and processing information stored in electronic devices (computers, mobile phones, tablets, memories, etc.). Such information may be protected by fundamental rights, to personal and family privacy, as well as the secrecy of communications.

Keywords

Inspection by the Tax Administration of content stored in an electronic device.

Cómo referenciar: Gandarias Cebrián, L. (2023). Registro por la Administración Tributaria del contenido almacenado en un ordenador personal: requisitos que deben reunir tanto la solicitud como la autorización judicial: STS de 29 de septiembre de 2023, Rec. núm. 4542/2021. *Revista Técnica Tributaria* (143), 251-261

SUMARIO

1. Doctrina del tribunal

Solicitud de registro referida al contenido almacenado en un ordenador personal: requisitos que deben reunir tanto la solicitud como la autorización judicial. La doctrina legal sentada por la Sección Segunda de la Sala Tercera del Tribunal Supremo en relación con las exigencias de la autorización de acceso y entrada a domicilios constitucionalmente protegidos –sujeción a los principios de necesidad, adecuación y proporcionalidad de la medida–, es extensible a aquellas actuaciones administrativas que tengan por objeto el acceso y tratamiento de la información almacenada en dispositivos electrónicos –ordenadores, teléfonos móviles, tabletas, memorias, etc.– que pueda resultar protegida por los derechos fundamentales a la intimidad personal y familiar y al secreto de las comunicaciones.

Tales exigencias, que deben ser objeto de un juicio ponderativo por el juez autorizante, no pueden basarse, exclusivamente, en el relato que realice la Administración en la solicitud, sin someter tal información a un mínimo contraste y verificación.

En todo caso, **el respeto a los derechos fundamentales –con máximo nivel de protección constitucional– prima sobre el ejercicio de potestades administrativas, máxime ante la falta de una regulación legal completa, directa y detallada.**

2. Supuesto de hecho

La cuestión que se ventila en la Sentencia objeto de este comentario se enfrenta a una situación singular, consistente, en el requerimiento realizado a un contribuyente en la sede de las oficinas de la inspección de la AEAT para que permitiera a la Unidad de Auditoría Informática realizar una copia de su ordenador portátil –que llevaba en todas las visitas consigo a fin de consultarlo–, con el fin de examinar la información con trascendencia tributaria contenida en el dispositivo. No consintiendo tal petición, los actuarios le informaron de que se iban a adoptar medidas cautelares al amparo del artículo 146 de la LGT, consistentes en la copia en un disco duro de la información del equipo portátil con el consiguiente precinto para su posterior apertura tras obtener autorización judicial. Alternativamente, caso de no permitir la copia, se procedería a la incautación y precinto del ordenador para su examen una vez obtenida autorización judicial, como de hecho sucedió, si bien es cierto que entre el copiado o volcado de datos y la solicitud judicial transcurrieron más de tres meses, aun contando con el trámite de medidas cautelares que lo precedió, lo que se califica –con fundamento– de una dilación injustificada e inexplicable, máxime si acontece con grave incidencia en derechos fundamentales, por más que se tratara de una copia.

A ello habría que añadir que el copiado se realiza finalmente, mediando una suerte de adhesión, que, al decir de la sentencia, se presta bajo cierta coacción,

pues ante la negativa del interesado a facilitar el ordenador que portaba, se le advierte de que le sería incautado –*tertium non datur*–; esto es, que el copiado era el mal menor que le esperaba, al que no se negó, lo que se pone de manifiesto mediante la aceptación forzada en las alegaciones. Si atendemos al régimen estatuido en la LECrim, para esa misma medida en un procedimiento criminal, lógicamente más gravoso, no cabría medida cautelar alguna antes de comunicarla al juez.

3. Fundamentos de derecho

La Sala estima que **las reglas de competencia y procedimiento que la ley procesal establece para la autorización judicial de entrada en domicilio constitucionalmente protegido**, a fin de llevar a cabo actuaciones de comprobación tributarias, son, *prima facie*, **inidóneas para autorizar el copiado, precinto, captación, posesión o utilización de los datos contenidos en un ordenador, cuando esa actividad se produce fuera del domicilio del comprobado y puede afectar al contenido de derechos fundamentales.**

Este pronunciamiento es trascendente porque se acude, como reflexión relevante, a la **posible aplicación subsidiaria del artículo 588 *sexies* de la LECrim., a falta de una completa y detallada regulación del contenido esencial de determinados derechos fundamentales y su incidencia en ellos por la Administración, objeto de rigurosa excepcionalidad y control, para dotar al ciudadano de unas garantías judiciales mínimas en esta clase de actuaciones tan intrusivas.**

Así, en relación con los derechos que se ven comprometido por la medida cautelar adoptada consistente en copiar el contenido del ordenador –artículo 146 de la LGT–, **cuya adopción no cabe cuando incide en el contenido esencial especialmente protegido por su condición de fundamentales**, al concebirse con tal rango el «entorno virtual», como algo distinto y nuevo respecto de los derechos afectados, conduce al límite jurídico estructural que figura en la LECrim., respecto del empleo de potestades más vigorosas e invasivas, como las penales frente al investigado.

Y ahí aparece un problema de dogmática jurídica: **ni la ley de la jurisdicción contencioso-administrativa ni la LOPJ fijan normas de competencia y procedimiento en relación con el precinto, incautación, volcado y examen de los datos de un dispositivo de gestión y almacenamiento –aquí, un ordenador portátil– que apodere al juez administrativo para autorizar la medida fuera del ámbito de la autorización de entrada en domicilio constitucionalmente protegido**, incluso en los términos establecidos a partir de la reforma operada por ley 11/2021, inaplicable *ratione temporis*.

Habría, pues, que preguntarse si los actos judiciales impugnados están amparados por atribución de competencia de alguna clase. **Dada, además, la afectación del contenido esencial de derechos fundamentales, debería existir una regulación, procedimental y sustantiva** que no sólo completase las muy embrionarias disposiciones sobre competencia y procedimiento que existen en nuestro ordenamiento positivo, sino que regulase de modo sustantivo los casos en que queda justificada la incidencia en un derecho fundamental, lo que afectaría no

sólo a las limitaciones legítimas de éste, en aras de la consecución de un fin constitucionalmente válido, sino a las atribuciones de la Administración y de los Tribunales de Justicia.

En todo caso, **la regulación –que no existe– para dirimir la cuestión con plenitud habría de tener rango de ley orgánica** –art. 81.1 de la CE–.

Al margen de ello, **la doctrina legal relacionada con las exigencias de la autorización de acceso y entrada a domicilios constitucionalmente protegidos –sujeción a los principios de necesidad, adecuación y proporcionalidad de la medida–, es extensible a aquellas actuaciones administrativas que tengan por objeto el conocimiento, control y tratamiento de la información almacenada en dispositivos electrónicos** –ordenadores, teléfonos móviles, tabletas, memorias, etc.– que pueda resultar protegida por los derechos fundamentales a la intimidad personal y familiar; al secreto de las comunicaciones y a la protección de datos –muy particularmente, sentencias de 10 de octubre de 2019, Rec. 2818/2017 y 1 de octubre de 2020, Rec. 2966/2019, dictadas por la Sección Segunda de la Sala Tercera del Tribunal Supremo–.

Tales exigencias, como ha quedado dicho, deben ser objeto de un juicio ponderativo por parte del juez autorizante, que no puede basarse, exclusivamente, en el relato que realice la Administración en la solicitud que dirija, sin someter tal información a un mínimo contraste y verificación.

Lo cierto es que **el respeto a los derechos fundamentales –con máximo nivel de protección constitucional– prima sobre el ejercicio de potestades administrativas, máxime ante la falta de una regulación legal completa, directa y detallada.**

Establecida esta doctrina, se resuelve que el auto y la sentencia objeto de enjuiciamiento casacional no observaron aquellas exigencias, a partir de la constatación de que el acceso íntegro e indiscriminado a los datos de contenido personal en un ordenador de tal índole, acordado antes de toda autorización judicial, vulnera los derechos constitucionales concernidos, como la intimidad personal y familiar, el secreto de las comunicaciones y la protección de datos de carácter personal.

Dada la naturaleza de la infracción, por la Administración primero y luego por los Tribunales, la actuación llevada a cabo es nula de pleno derecho, calificación que, fundada en el art. 217.1.a) de la LGT, deriva inexorablemente de la vulneración del contenido esencial de tales derechos fundamentales.

4. Análisis

En relación con la insuficiencia normativa para acceder al contenido de un ordenador personal, puede advertirse que el artículo 8.6 de la LJCA alude, *in fine*, a las autorizaciones para la entrada en domicilios y otros lugares constitucionalmente protegidos y, curiosamente, el artículo 91.2 de la LOPJ mantiene la competencia de los JCA, para la entrada en los domicilios y los restantes edificios o lugares cuyo acceso requiera el consentimiento de su titular, **cuando ello proceda para la ejecución forzosa de actos de la Administración**, dejando

la reforma introducida por conducto de la Ley 11/2021 incompleta en este aspecto esencial.

Por ello, es lógico abordar esta materia partiendo, como hace la sentencia en un ejercicio de integración ciertamente encomiable, en lo que califica de reflexión no irrelevante, aludiendo a la posible aplicación subsidiaria del art. 588 *sexies* de la LECrim., a falta de una completa y detallada regulación del contenido esencial de determinados derechos fundamentales y su incidencia en ellos por la Administración, objeto de rigurosa excepcionalidad y control, para dotar al ciudadano de unas garantías judiciales suficientes en esta clase de actuaciones que, ocioso es mencionarlo, resultan muy invasivas.

La sentencia acude, para justificar este planteamiento, al derecho fundamental al entorno virtual como algo distinto y nuevo respecto de los derechos concernidos, lo que permite considerar que la reforma operada en la LECrim. de 2015 y la jurisprudencia constitucional y del TS (Sala 2ª) sobre la materia, refuerzan la limitación de la intervención en estos derechos fundamentales, en tanto derivados del conocimiento indiscriminado del contenido de dispositivos informáticos.

Esta apreciación sobre el derecho a un entorno virtual o digital, con la que coincide quien suscribe, ha podido generar cierta confusión, por su extraordinaria complejidad, al no interpretarse correctamente la esencia de los derechos del artículo 18 de la CE, que se han resumido en una noción basilar: la de «***ser dejado en paz».***

Repárese, como apreciación inicial, en que los artículos 588 sexies a, y 588 sexies b, de la LECrim, reguladores de la diligencia de acceso a un dispositivo de almacenamiento masivo de información, distinguen entre que el dispositivo que eventualmente pudiera contener información relevante –con trascendencia tributaria, por lo que nos toca– sea encontrado dentro de un lugar susceptible de ser considerado como domicilio, o fuera de aquel, sin establecer regulación alguna en relación con el derecho a la inviolabilidad domiciliaria, de donde se desprende que una cosa es poder acceder al interior de un inmueble que goce de protección constitucional, contando para ello con la autorización judicial oportuna, y otra muy distinta que ello permita sobreentender que el salvoconducto conlleva, adicionalmente, la facultad de apoderarse y examinar el contenido de los dispositivos encontrados en su interior, lo que exigiría una autorización específica, sin despreciar, a mayor abundamiento, que estamos ante un ámbito extensible a la información alojada en la nube y en redes virtuales.

La prohibición expresa establecida en el artículo 588 sexies a], párrafo segundo, de la LECrim delimita las diligencias previstas dentro del Capítulo I, perfilando el contenido de cada uno de los derechos del artículo 18.1 y 2 de la CE, tal y como pone de manifiesto la Circular de la Fiscalía General del Estado –CFGE– 5/2019, de 6 de marzo, págs. 55 y 56.

En este entorno cabe integrar el derecho al secreto de las comunicaciones, recogido en el artículo 18.3 de la CE, cuyo ámbito de protección alude al proceso de comunicación y a los que en él intervienen –STC 114/1984–, de modo que su infracción no puede descartarse en la intervención de un ordenador, particularmente, es cierto, cuando se realiza de forma remota, pero sin que puedan

descartarse otras hipótesis al conectar cualquier dispositivo para visionar su contenido, de ahí que la CFGE 5/2019, de 6 de marzo, estime que la diligencia de registro remoto de equipos está a medio camino entre el registro de dispositivos de almacenamiento y la intervención de comunicaciones.

Es cierto que un procedimiento de comunicación «en marcha» –que es el que protege el derecho al secreto de las comunicaciones– no es equiparable a uno culminado, tutelado por los derechos a la intimidad, la privacidad o en su caso, la autodeterminación informativa, pero, siendo improbable, no puede rechazarse *a priori* que su conexión afecte a comunicaciones en curso, debiendo preverse esta posibilidad en el auto habilitante que acuerde el acceso al dispositivo expresamente.

Puede apreciarse que el tradicional análisis de los derechos fundamentales desde una dimensión individual o diversa pierde fuerza frente a situaciones de mucha mayor complejidad, sin que ello suponga acudir a una creatividad propia de la *nouvelle cuisine*, sino a la **consolidación de una evolución conectada a la problemática jurídica inherente al uso de dispositivos e instrumentos electrónicos de almacenamiento y tratamiento de datos que conduce a un análisis de los derechos establecidos en el artículo 18 de la CE desde una óptica unitaria**, que es precisamente la que ha dado lugar al reconocimiento del **derecho al entorno virtual** al que se refiere con acierto la sentencia objeto de este comentario. Se trata, como ha puesto de manifiesto la literatura especializada, de abordar la materia desde una dimensión o visión colectiva en la forma de entender todos los derechos del artículo 18 de la CE.

Expresado en otros términos, el abordaje consistiría en reconocer que un ordenador, o cualquier dispositivo análogo, sirve para realizar tareas profesionales pero también actividades personales susceptibles de generar datos expresados en un lenguaje informático capaces de crear un perfil del usuario –su imagen virtual– que conecta igualmente con el apartado 4 del artículo 18 de la CE –*«la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*–, originando un derecho a ser protegido del uso por parte de terceros de esos datos –de esa imagen– inherente al ejercicio pleno de todos los derechos individuales.

Siendo innegable que los datos que se encuentran contenidos en un dispositivo están protegidos por los diferentes derechos fundamentales establecidos en el artículo 18 de la CE, hay que admitir la dificultad de diferenciar entre unos y otros, lo que sugiere **una tutela integral –una protección conjunta, si se prefiere– conducente a la custodia de los perfiles digitales de cada persona mediante el derecho al propio entorno virtual o digital reconocido por conducto jurisprudencial** –cfr. por otras muchas, SSTS núm. 342/2013, de 17 de abril y la STS núm. 786/2015, de 4 de diciembre, de las que ha sido ponente Manuel Marchena Gómez–, tanto más cuando este entorno escapa al control personal del sujeto, en tanto se conforma con la recopilación de los datos generados por el uso diverso de los dispositivos electrónicos, creando un rastro electrónico –muchas veces inconsciente– que abarca los diferentes derechos del artículo 18 de la CE.

La Fiscalía General del Estado reconoce el derecho dimanante de esta doctrina y al analizar los derechos que se ven afectados por las diligencias de inves-

tigación electrónica, destacan el «*tratamiento unitario de los derechos comprometidos*» –CFGE 5/2019, de 6 de marzo, pág. 4–.

Puede afirmarse, por tanto, que se trata de un **derecho fundamental reconocido por la jurisprudencia –particularmente en el ámbito penal–, que protege los datos generados por el uso masivo de dispositivos electrónicos, sin perjuicio del derecho fundamental que ampare a cada caso individualmente.** Así, desde una perspectiva procesal, el derecho al propio entorno virtual permite un tratamiento homogéneo que supera las dificultades derivadas de la divergencia entre las previsiones constitucionales, individualmente consideradas, y los modos y medios de hacer efectivos los límites de su contenido, habilitando al juez de garantías encargado de autorizar medidas intrusivas a determinar con precisión su alcance, sin desconocer la doctrina ni la jurisprudencia sobre cada derecho fundamental de los establecidos en el artículo 18 de la CE, sino completándola con una visión más amplia cuando se sobreponen o entreveran cuando el registro se realiza en un dispositivo electrónico en relación con el que pueden concurrir o verse afectados distintos derechos contenidos en el artículo 18 de la CE.

De esta forma, **no se rechazan la doctrina y la jurisprudencia concernientes a cada derecho fundamental aisladamente considerado, sino que, como con acierto ocurre en la sentencia objeto de estas líneas, se realiza un análisis completo del fenómeno atendiendo con rigor a las circunstancias concurrentes, con los instrumentos normativos de los que se dispone, *ratione materiae***.

Repárese que se trata de ponderar la efectividad del deber de contribuir, mediando una actividad inspectora especialmente vigilante y eficaz, aunque pueda resultar a veces incómoda y molesta –STC 110/1984– y el escrupuloso respeto a los derechos fundamentales concernidos, ante los que aquella debe plegarse, máxime, como recuerda la sentencia comentada, ante la falta de una regulación legal completa, directa y detallada. Escuchemos al TS –sin perjuicio de recomendar encarecidamente su lectura completa, por su sensibilidad y el carácter garantista de los derechos del obligado tributario que se advierten en el pronunciamiento–: «*Desde la perspectiva normativa, hay otra cuestión susceptible, al menos, de reflexión: si las exigencias materiales y formales que el art. 588 sexies, a), b) y c) de la LECrim., en la redacción dada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la expresada ley para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, impone como reglas limitativas de las potestades de intervención en manos del juez de instrucción en una causa abierta por delito, son también preceptivas para el juez administrativo en defecto de norma aplicable, pues si el registro o captación de datos contenidos en dispositivos electrónicos está sujeto a estrictas garantías y formalidades en favor del investigado penal –cuya posición, por fuerza, ha de ser más aflictiva–, en mayor medida deberían operar, al menos como límite, en el seno de una comprobación meramente administrativa, a fin de no hacer de peor condición al ciudadano en su calidad de comprobado fiscal que al encausado penal.*»

Así, siguiendo tanto la normativa como la doctrina procesal-penal en la línea descrita, **la incautación un dispositivo electrónico, tanto dentro como fuera del domicilio del investigado, no legitima el acceso a su contenido, sin perjuicio**

de que pueda ser autorizado por el juez competente con todas las garantías de adecuación, necesidad y proporcionalidad inherentes a este tipo de intervenciones –siempre de carácter subsidiario–, pudiendo ser valoradas conjuntamente en una sola resolución que acuerde la entrada y registro en un domicilio constitucionalmente protegido y el acceso a los dispositivos electrónicos que se hallen en aquel, mediando, eso sí, tanto una motivación como los pronunciamientos expresos referidos a cada uno de los aspectos determinantes de la actuación de que se trate.

Son muchos los matices que admite este derecho al entorno virtual, claro está, como puede advertirse en la jurisprudencia penal que se ha ocupado de su tratamiento en la que se afirma que su protección se puede limitar ante razones justificadas y debidamente ponderadas, siendo el contenido del art. 588 bis a] de la LECrim el que determina los principios y aspectos que deben tenerse en cuenta a la hora de valorar la adopción de alguna diligencia en la que este derecho sea aplicable –cfr. STS núm. 500/2022, de 24 de mayo, de la que ha sido ponente Antonio del Moral–.

Todo en el bien entendido de que **la limitación al derecho al entorno virtual también debe ser valorada caso a caso:** «*frente a lo que sucede respecto del contenido material de otros derechos, el derecho a la intimidad o, si se quiere, el espacio de exclusión que frente a otros protege el derecho al entorno virtual, es susceptible de ampliación o reducción por el propio titular. 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. Desde luego, son imaginables usos compartidos de dispositivos de esa naturaleza en los que se impongan reglas de autolimitación que salvaguarden el espacio de intimidad de cada uno de los usuarios.*» –STS núm. 287/2017, de 19 de abril, de la que ha sido ponente Manuel Marchena–.

Quedémonos con que «*El legislador opta por reforzar las garantías y dar un tratamiento unitario a los datos contenidos en estos dispositivos ante el riesgo de eventuales excesos. Se acuña así el término 'derecho a la protección del entorno virtual' como derecho constitucional de nueva generación. (STS N.º 204/2016 de 10 de marzo). Y que ampara toda la información en formato electrónico que a través del uso de las nuevas tecnologías va generando el usuario (huella digital). **Este reforzamiento supone, por ejemplo, la necesidad, entonces, de exteriorizar en un razonamiento diferenciado por el Juez que, además de la inviolabilidad del domicilio, es necesario hacerlo también de otros derechos mediante el registro de estos dispositivos, aunque sean hallados en un registro judicial, autorización que puede darse en el mismo auto de entrada o posteriormente».*** –SAP de Cádiz núm. 335/2017, de 29 de diciembre–.

Parece evidente la relevancia de la tendencia, mediante el uso de esta doctrina, a proteger **el acceso a los datos personales que se encuentran en un dispositivo de almacenamiento masivo de información**, donde quiera que aquel se encuentre, reservando al juez, actualmente sin instrumentos normativos suficientes en el ámbito contencioso-administrativo, al contrario de lo que ocurre en el proceso penal, la posibilidad de conceder el acceso, salvaguardando la

afectación de cualquiera de los derechos del artículo 18 de la CE, **sustrayendo cualquier decisión sobre esos aspectos a cualquier autoridad administrativa.**

Esta concepción, qué duda cabe, patrocina un máximo respeto por los derechos del contribuyente afectado por la medida de que se trate, como ha quedado demostrado en la sentencia cuyo comentario alcanza a su término, extensible –en opinión de quien suscribe–a terceros que puedan verse implicadas por su adopción –piénsese en empleados de una empresa o en familiares en los casos de uso compartido de los dispositivos, etc.–, al someter al control judicial la oportunidad y necesidad de limitar estos derechos, mediante una adecuada valoración de todos los aspectos en juego –y en riesgo–, quedando efectivamente reforzado el artículo 18 de la CE en su conjunto.

Queda claro, sin perjuicio de lo expuesto, que los requisitos para permitir una entrada domiciliaria, forjados en una consistente doctrina legal armada en la Sección Segunda de la Sala Tercera del Tribunal Supremo, deben proyectarse sobre la captación o copiado de datos, ponderando si la necesidad, adecuación o proporcionalidad son compatibles con el copiado indiscriminado de todos los datos, incluso personales o íntimos o, en todo caso, debe seleccionarse desde el primer momento la información que se precisa, por su relevancia tributaria, para proseguir la comprobación, sin copiar, precintar –o adoptar medidas cautelares, proscritas cuando afectan a derechos fundamentales– en relación con la información sin trascendencia tributaria, al margen de la incidencia o no, para cada archivo, en algún derecho fundamental, como la intimidad o privacidad o, incluso, el secreto de las comunicaciones, quedando prohibida la captación de archivos o datos ajenos a la función comprobadora, **resultando que lo relevante es siempre el respeto al contenido de esos derechos que podrían verse afectados por el registro de esos datos, con independencia de que su ubicación sea física o virtual.**