



## **Documento de trabajo**

### **SEMINARIO PERMANENTE DE CIENCIAS SOCIALES**

# **CRITERIOS PARA COMPATIBILIZAR EL DERECHO DE ACCESO Y LA PROTECCIÓN DE DATOS POR LAS ADMINISTRACIONES PÚBLICAS**

**María Lidón Lara Ortiz**

**SPCS Documento de trabajo 2019/4**

<https://www.uclm.es/Cuenca/CSociales/publicaciones/inicio>

© de los textos: sus autores.

© de la edición: Facultad de Ciencias Sociales de Cuenca.

Autora:

María Lidón Lara Ortiz

[mlara@uji.es](mailto:mlara@uji.es)

Edita:

Facultad de Ciencias Sociales de Cuenca  
Seminario Permanente de Ciencias Sociales

Codirectoras:

Pilar Domínguez Martínez

María Cordente Rodríguez

Silvia Valmaña Ochaita

Avda. de los Alfares, 44

16.071–CUENCA

Teléfono (+34) 902 204 100

Fax (+34) 902 204 130

<https://www.uclm.es/Cuenca/CSociales/publicaciones/inicio>

I.S.S.N.: 1887-3464 (ed. CD-ROM)

D.L.: CU-532-2005

Impreso en España – Printed in Spain.

# CRITERIOS PARA COMPATIBILIZAR EL DERECHO DE ACCESO Y LA PROTECCIÓN DE DATOS POR LAS ADMINISTRACIONES PÚBLICAS

**María Lidón Lara-Ortiz<sup>1</sup>**

*Profesora Ayudante Doctora de Derecho Administrativo*

*Universitat Jaume I*

## RESUMEN

El derecho de acceso a la información pública es una de las manifestaciones de la transparencia de las Administraciones Públicas que descansa sobre el artículo 105.b) de la Constitución española. Sin embargo, este derecho se ejerce por los ciudadanos con las limitaciones contempladas en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que concibe la protección de datos personales como uno de los límites más relevantes de aquel derecho de los ciudadanos.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales impone a la actividad de las Administraciones Públicas la protección de estos datos personales al igual que ocurre en su tratamiento por los particulares, pero el cumplimiento de las obligaciones de la actuación administrativa transparente hacen necesaria una ponderación de la extensión del derecho de acceso a los expedientes e información pública, y de la amplitud de la protección que se debe dispensar a dichos datos personales.

El hecho de que las Administraciones públicas tengan como principal finalidad la defensa de los intereses generales, matiza el derecho a la protección de datos y requiere una especial compatibilización con otros derechos y situaciones jurídicas que se generan con ocasión de la actividad administrativa.

En este trabajo se pretenden determinar las bases de la extensión del derecho a la protección de datos de los ciudadanos en su tratamiento por las Administraciones públicas, al tramitar procedimientos administrativos y realizar otras actividades que les son propias. Con tal finalidad, se exponen los criterios que deben ser tenidos en cuenta en la determinación de la preferencia de la protección de datos personales o de la

---

<sup>1</sup> mlara@uji.es

transparencia administrativa, y se valora cómo mejorar la regulación existente en la actualidad.

**Palabras clave:** Protección de datos, Derecho de acceso, Buena administración, Administraciones Públicas, transparencia administrativa.

**Indicadores JEL:** K23.

## ABSTRACT

The right to access to public information is one of the manifestations of the transparency of Public Administrations that lies on article 105.b) of the Spanish Constitution. However, this right is exercised by citizens with the limitations contained in the Act number 19 of 2013, of December 9, on transparency, access to public information and good governance, which conceives the protection of personal data as one of the most relevant limits of that right of citizenship.

The Organic Act number 3 of 2018, of December 5, on the Protection of Personal Data and guarantee of digital rights, imposes the protection of these personal data to the Public Administrations activity as it does in their treatment by individuals, but compliance with the obligations of transparent administrative action requires a weighting of the extension of the right of access to public records and information and the extent of protection that should be provided to such personal data.

The fact that public administrations aim to defence general interests, crashes to some extent to data protection, and it needs a special compatibility with other rights and legal situations that are related to the activity of administrative activity.

This paper aims to assess the basis of the extension of the right to protection of citizens in the treatment of public administrations, the processing of administrative procedures and while performing other activities that are in their scope of action. With this purpose, we analyse the criteria that must be taken into account in determining the preference of personal data protection or administrative transparency, and we assess how to improve the current regulations.

**Key words:** Personal data protection, the right to access to the public files, the right to good administration, Administrations' transparency.

**JELcodes:** K23.

## 1. INTRODUCCIÓN

La actividad de las Administraciones Públicas requiere de la gestión de datos personales de los ciudadanos, y a pesar de que la regulación de la protección de datos las vincula del mismo modo que a los particulares, el hecho de que las Administraciones Públicas tengan como principal propósito la defensa de los intereses generales, y deban cumplir ciertos deberes de transparencia para posibilitar el control democrático de su actividad, genera ciertos conflictos entre la protección de los datos personales tratados por ellas y su obligación de ser transparentes<sup>2</sup>.

La transparencia administrativa impone la obligación de comunicar o difundir, y hacer accesible la información de la actividad de las Administraciones públicas de conformidad con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y con las leyes autonómicas dictadas por los gobiernos autonómicos para regula la transparencia en el ámbito de sus competencias territoriales. Tales normas delimitan la extensión de la transparencia a aquellas informaciones que se estiman de interés para los ciudadanos. Para algunos autores, la protección de datos personales actúa como un auténtico límite de dicha transparencia, mientras que, para otros autores, es una garantía de la autonomía de los ciudadanos frente al poder público<sup>3</sup>.

Debemos poner de relieve que la transparencia administrativa, al permitir conocer los pormenores de la actuación administrativa en diversos ámbitos, es una manifestación de la buena administración, y como tal, es indicativo de un mayor grado del funcionamiento democrático de las instituciones, ya que permite a los ciudadanos tener un papel mucho más activo respecto de las cuestiones públicas<sup>4</sup>, y es una

---

<sup>2</sup> Diversos autores han puesto de relieve la confrontación de ambos derechos, entre ellos: PIÑAR MAÑAS J.L. (dir.), (2014), *Transparencia, acceso a la información y protección de datos*, Ed. Reus; y GUICHOT E. (2007), “Acceso a la información en poder de la Administración y protección de datos personales”, en *Revista de Administración Pública*, núm. 173, Ed. Instituto Nacional de Administración Pública, Madrid.

<sup>3</sup> ARENA G., (1997), “La transparencia administrativa”, *Documentación Administrativa / n.º 248-249 (mayo-diciembre 1997)*, Instituto Nacional de Administración Pública, Madrid, p.397.

<sup>4</sup> ÁVILA RODRÍGUEZ, C.M. (2009), “El derecho ciudadano a una Buena Administración”, in Gutiérrez Rodríguez F.J. (Dir.), *El derecho de la ciudadanía a una Buena Administración. La Administración Electrónica*, Diputación de Málaga, Málaga, p. 31; JEGOUZO I., (1994), “El derecho a la transparencia administrativa: el acceso de los administrados a los documentos administrativos”, *Documentación Administrativa / n.º 239 (julio-septiembre 1994)*, Instituto Nacional de Administración Pública, Madrid, p. 12.

herramienta para controlar las resoluciones arbitrarias<sup>5</sup>, siendo considerado un requerimiento de buena gobernanza elevado al grado de Derecho Fundamental de los ciudadanos en el artículo 41 de la Carta de Derechos Fundamentales de la Unión Europea.

## 2. LA NATURALEZA JURÍDICA DE LOS DERECHOS EN CONFLICTO

La protección de datos personales está vinculada con el Derecho Fundamental a la intimidad personal y familiar, reconocido como tal en todas las Constituciones europeas y en la Declaración Universal de Derechos Humanos (artículo 12). Además, la protección de datos personales, está reconocido como un Derecho Fundamental autónomo en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea<sup>6</sup>.

Por otro lado, el acceso a los registros públicos, como manifestación de la transparencia administrativa, forma parte del derecho a la buena administración, también reconocido como un Derecho Fundamental en el artículo 41.2 de la Carta de Derechos Fundamentales de la Unión Europea.

Inicialmente, estos derechos se incluyeron en la frustrada Constitución europea, manifestación de un emergente derecho constitucional de la Unión Europea, al que se refiere el artículo 6.2 del Tratado de Funcionamiento de la Unión Europea<sup>7</sup>. Más adelante, la Carta de Derechos Fundamentales de la Unión Europea, inicialmente proclamada en el Tratado de Niza, en el año 2000, fue objeto de revisión, con ocasión de la firma del Tratado de Lisboa, en 2007, entrando en vigor el 1 de diciembre de 2009, convirtiéndose en vinculante, en ese momento, para los Estados Miembros de la Unión Europea.

Como consecuencia de todo ello, los derechos incluidos en la misma deben ser considerados Derechos Fundamentales en el sistema legal de cada uno de los Estados Miembros. Como tales, además, son aplicados como principios del derecho de la Unión

---

<sup>5</sup> GIMENO FELIU J.M., (2017), “La transposición de las directivas de contratación pública en España: una primera valoración de sus principales novedades”, *Documentación Administrativa, Nueva Época – N° 4, Enero-Diciembre 2017*, Instituto Nacional de Administración Pública, Madrid, p. 10.

<sup>6</sup> RODOTÀ S. (2003), “Democracia y protección de datos”, *Cuadernos de Derecho Público, núms. 19-20 (mayo-diciembre 2003)*, Instituto Nacional de Administración Pública, Madrid, p. 17.

<sup>7</sup> TOMÁS MALLÉN B. (2004), *El derecho fundamental a una buena administración*, editado por Instituto Nacional de Administración Pública, Madrid, p. 31.

Europea, como declaró la Sentencia del Tribunal de Justicia de la Unión Europea en el caso C-274/99, de 6 de marzo de 2001<sup>8</sup>. Al considerarse principios del derecho de la Unión Europea, pueden ser citados ante los juzgados y tribunales de todos los Estados Miembros<sup>9</sup>.

La ponderación de los dos derechos requiere la anterior determinación de la relevancia de cada uno de estos derechos, evaluando la naturaleza jurídica de cada uno de ellos, así:

-La protección de los datos personales tienen su especial reconocimiento como Derecho Fundamental en la Unión Europea, pero no es reconocido como Derecho Humano. Sin embargo, y a pesar de su carácter autónomo del derecho a la intimidad, es innegable que puede apreciarse cierta conexión con el mismo, el cual sí está reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos, al declarar que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación”, al igual que en el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, que reconoce el Derecho Fundamental a la intimidad personal y familiar. El vínculo con el artículo 12 de la Declaración Universal de Derechos Humanos ha sido aplicada por diversos Estados con la finalidad de fundamentar algunas regulaciones sobre la autodeterminación informativa (como es el denominado, *habeas data*), como lo hicieron Suecia y Alemania<sup>10</sup>. Mientras, otros Estados Europeos, han fundamentado su regulación a la protección de datos directamente en el derecho a la intimidad, como Holanda y Finlandia<sup>11</sup>.

- El derecho de acceso a los expedientes administrativos está relacionado con el Derecho a la buena administración, y está reconocido en el artículo 41.2 de la Carta de Derechos Fundamentales de la Unión Europea, aunque no está incluido en la Declaración Universal de Derechos Humanos de 1948. Algunos autores mantienen que entre los Derechos Humanos y Derechos Fundamentales existe cierta identidad, de

---

<sup>8</sup> PIÑAR MAÑAS J.L. (2003), “El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, p. 55.

<sup>9</sup> MEILÁN GIL J.L. (2013), “La buena administración como institución jurídica”, en *Revista Andaluza de Administración Pública*, núm. 87, Sevilla, p. 14.

<sup>10</sup> RIBAGORDA GARNACHO A. (2008), “La protección de datos personales y la seguridad de la información”, *Revista Jurídica de Castilla y León*, n.º 16, septiembre 2008, Junta de Castilla y León, León, p. 377.

<sup>11</sup> TRONCOSO REIGADA A. (2003), “La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, p.235.

modo que asimilan los Derechos Fundamentales de primera generación a los Derechos Humanos contenidos en la Declaración de 1948, ya que constituyen el núcleo duro de los Derechos Humanos, considerándose este concepto como intercambiable y equivalente con el de los derechos Fundamentales<sup>12</sup>. Siguiendo esta tesis, el Derecho a la Buena Administración sería mucho más que un Derecho Fundamental, ya que también debería ser considerado como un Derecho Humano, al haber sido incorporado a la Carta de Derechos Fundamentales de la Unión Europea, todo ello desde la óptica que concibe ambos conceptos como intercambiables. Sin embargo, esta tesis no está admitida por completo, ya que otros autores mantienen que no son conceptos equivalentes<sup>13</sup>. El Tribunal Europeo de Derechos Humanos y la Corte Internacional de Derechos Humanos han reconocido la equivalencia de los conceptos “Derecho Humano” y “Derecho Fundamental”.

Como vemos, la naturaleza jurídica de los derechos en conflicto debe considerarse equivalente, o aunque no se mantenga la tesis que entiende que Derechos Humanos y Fundamentales son conceptos intercambiables, cualquiera de los dos es, sin ninguna duda, un derecho de relevancia especialmente cualificada, cualificación que incide al establecer criterios de prevalencia cuando ambos están en conflicto.

### **3. LA INCIDENCIA DE LOS AVANCES TECNOLÓGICOS EN LA GESTIÓN DE DATOS**

El tema que nos ocupa ha ganado relevancia en las últimas décadas, ya que no se puede negar que los medios telemáticos y electrónicos hacen más accesible todo tipo de información, así como facilitan el cumplimiento de ciertos deberes de transparencia por parte del sector público, incluso se han habilitado medios electrónicos para que las Administraciones y los ciudadanos se comuniquen<sup>14</sup>. Pero ello aumenta el riesgo de mostrar, difundir, o comunicar datos protegidos, como bien se ha puesto de relieve recientemente el Considerando número 8 de la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y

---

<sup>12</sup> AGUILAR CAVALLO G. (2010), “Derechos Fundamentales-Derechos Humanos. ¿Una distinción válida en el siglo XXI?”, *Boletín Mexicano de Derecho Comparado*, número 127, pp. 62-63.

<sup>13</sup> MARTÍN-RETORTILLO BAQUER L., (2006), *Vías concurrentes para la protección de los derechos humanos*, Thomson Reuters-Civitas, Navarra, p. 47.

<sup>14</sup> ACED FÉLEZ E., (2008), *Protección de Datos y e-Administración*, Agencia de Protección de Datos de la Comunidad de Madrid, Madrid, p.1.

la reutilización de la información del sector público, que modifica sustancialmente la anterior Directiva 2003/98/CE del Parlamento Europeo y del Consejo<sup>15</sup>.

El incremento del riesgo a difundir datos protegidos requiere una adecuada regulación de su gestión, y la delimitación de los casos en que su difusión o comunicación está justificada, siendo esta una de las cuestiones que ha generado una preocupación creciente en los últimos años. Esta preocupación ha sido recogida en diferentes textos e instrumentos jurídicos de la Unión Europea, entre ellos, el Dictamen del Comité Económico y Social Europeo sobre «La revolución digital teniendo en cuenta las necesidades y los derechos de los ciudadanos», número 2019/C 190/03, que pone de relieve los riesgos más relevantes derivadas de la digitalización en los ámbitos de la autonomía, la responsabilidad, la seguridad, la dignidad y la privacidad personal. Las consecuencias, desde el punto de vista normativo, de esta ingente preocupación, son palpables en la regulación sectorial de diversas materias, y en otras normas generales como el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»), y como la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público. Todas estas normas convergen con las normas reguladoras de la protección de datos personales, y deben ser tenidas en cuenta en la aplicación de su normativa específica.

Un factor que debe ser considerado para mejorar la actual protección de datos de los ciudadanos es la de informarles sobre cómo defender su derecho frente a las

---

<sup>15</sup> En este sentido, el referido Considerando 8 de la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, fundamenta la necesidad de regular la gestión de datos por el sector público del siguiente modo “El sector público de los Estados miembros recoge, produce, reproduce y difunde una amplia gama de información en numerosos ámbitos de actividad, como el social, político, económico, jurídico, geográfico, medioambiental, meteorológico, sísmico, turístico, empresarial, educativo y de las patentes. Los documentos elaborados por los organismos del sector público de carácter ejecutivo, legislativo o judicial constituyen un conjunto amplio, diverso y valioso de recursos que pueden beneficiar a la sociedad. Ofrecer esta información, que incluye los datos dinámicos, en un formato electrónico de uso habitual permite que los ciudadanos y las personas jurídicas hallen nuevas formas de utilizarla y creen productos y servicios nuevos e innovadores. Los Estados miembros y los organismos del sector público pueden beneficiarse y recibir un apoyo financiero adecuado de los fondos y programas de la Unión pertinentes, garantizando un uso generalizado de las tecnologías digitales o la transformación digital de las administraciones públicas y los servicios públicos en su empeño por facilitar la reutilización de los datos”.

Administraciones, para exigir, el respeto a sus derechos, cuando proceda, lo que implica un conocimiento de los límites de tal derecho<sup>16</sup>, de los casos en que éste cede frente a la transparencia administrativa en sus diversas manifestaciones, y de los mecanismos para reclamar tal respeto, lo que requiere una progresiva toma de conciencia del carácter fundamental del Derecho a la protección de datos personales<sup>17</sup>.

#### **4. LA REGULACIÓN DE LA PROTECCIÓN DE DATOS TRATADOS POR LAS ADMINISTRACIONES PÚBLICAS**

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno hace referencia a la protección de datos por parte de las Administraciones al cumplir sus obligaciones de transparencia de conformidad con lo previsto en ella, estableciéndose reglas especiales en determinados casos, pues la norma adelanta una ponderación de los derechos en conflicto y determina la prevalencia de uno sobre otro de forma preordenada<sup>18</sup>.

Conforme a la misma, si la información solicitada en el ejercicio del derecho de acceso contiene datos personales que revelen la ideología, la filiación, la religión o las creencias, el acceso a los mismos sólo se considera autorizado si se cuenta con el consentimiento expreso y por escrito de la persona afectada, salvo que el dato se hubiera hecho público de forma evidente antes de que se solicite el acceso a la misma.

En el caso de que la información incluya datos especialmente protegidos relativos a la comisión de infracciones penales o administrativas o datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual que no conllevaran la amonestación pública al infractor, el acceso sólo se podrá autorizar en

---

<sup>16</sup> CERVERA NAVAS L. (2003), “El modelo europeo de protección de datos de carácter personal”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, p. 142.

<sup>17</sup> CALVO ROJAS E., (2003), “Algunas consideraciones sobre el procedimiento sancionador en el ámbito de la protección de datos personales”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, p. 230.

<sup>18</sup> Se han realizado diversos estudios de los criterios que contiene el artículo 15 de la Ley de Transparencia para delimitar la prevalencia de esta o de la protección de datos, es el caso de: FERNÁNDEZ RAMOS S. (2017), “Acceso a la información pública versus protección de datos personales”, *Revista española de Derecho Administrativo*, núm. 184; y de RODRIGUEZ ÁLVAREZ J.L. (2016), “Transparencia y protección de datos personales: criterios legales de conciliación”, en CANALS AMETLLER (ed.), *Datos, Protección, Transparencia y Buena Regulación*, ed. Documenta.

caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley.

En todos los casos, el consentimiento implícito no puede ser considerado a efectos de autorizar la comunicación de los datos personales<sup>19</sup>.

Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público que impida la divulgación, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal. Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

- El menor perjuicio a los afectados y a los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.
- La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.
- La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

Estos criterios no serán aplicables si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas, pudiéndose cumplir de este modo, las obligaciones de transparencia. En otro

---

<sup>19</sup> Agencia Española de Protección de Datos (2018), *Informe respondiendo a la consulta sobre el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*, Agencia Española de Protección de Datos, España, p. 2.

caso, si procede su aplicación, la normativa de protección de datos personales será de aplicación también al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

Junto con los criterios establecidos por la Ley de Transparencia, se deben tener en cuenta las reglas que dimanen de la normativa sobre protección de datos y que son, esencialmente, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que fue poco aplicada por los Estados Miembros, por lo que su sustitución por el Reglamento UE de 2016 pretende una mayor efectividad de la normativa europea<sup>20</sup>, y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Poniendo en relación estas normas, pueden ser extraídos algunos criterios que actúan como límites, o al menos matizan la extensión del derecho de acceso, ponderando el derecho a la protección de datos personales. Así:

- Principio de licitud o legitimidad. La exhibición de datos es lícita si media consentimiento del titular de los datos o se hace en cumplimiento de obligaciones contractuales o legales, o para proteger intereses vitales, públicos o satisfacer intereses legítimos. Las causas de legitimidad están basadas en las funciones del gestor de los datos, con origen en la ley, un contrato, o el consentimiento expreso<sup>21</sup>.
- Principio de información o transparencia. La transparencia se aplica en relación con la entrega de información que afecte al propio interesado tanto si los datos fueron entregados por él como si se hubieran obtenido de otra fuente.
- Principio de minimización de datos o proporcionalidad. La extensión de los datos mostrados debe limitarse a lo necesario y adecuado para cumplir los fines de la

---

<sup>20</sup> CAZURRO BARAHONA V. (2008), “La protección de datos y los medios de comunicación”, *Revista Jurídica de Castilla y León*, n.º 16, septiembre 2008, Junta de Castilla y León, León, p. 232.

<sup>21</sup> GUASCH PORTAS V. AND SOLER FUENSANTA J.R. (2015), “El interés legítimo en la protección de datos”, *Revista de Derecho UNED*, núm. 16, Universidad Nacional de Estudios a Distancia, Madrid, p. 419.

transparencia administrativa en el caso concreto. Este criterio se ha recogido en algunas normas especiales en sentido similar, como por ejemplo, en el Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, que regula la publicidad edictal de sanciones de tráfico en su artículo 92, como posibilidad facultativa para realizar la publicación sustitutiva a la notificación fallida, que en caso de hacerse debe mostrar los mínimos datos posibles<sup>22</sup>.

- Principio de limitación de la finalidad. El uso de los datos queda limitado al motivo por el que se entregaron, de modo que su uso posterior para una finalidad diferente a la originaria no está justificada. Este criterio se ajusta a la interpretación finalista del sistema de transparencia administrativa, según la cual la difusión de información se justifica en el cumplimiento de su propio objetivo<sup>23</sup>.
- Principio de exactitud de los datos. Las Administraciones públicas deben poder verificar la exactitud de los datos que tratan.
- Principio de limitación del plazo de conservación (derecho al olvido). Los datos personales no deben conservarse más tiempo del necesario para los fines del tratamiento.
- Principio de integridad o seguridad. Es necesario que las Administraciones públicas garanticen la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.
- Principio de confidencialidad. Las Administraciones tienen deber de guardar confidencialidad respecto a los datos personales que traten, siendo una obligación complementaria a la de guardar secreto profesional que tiene un carácter más general.

---

<sup>22</sup> GAMERO CASADO E. (2009), “El régimen de notificaciones: la dirección electrónica vial (DEV) y el tablón edictal de sanciones de tráfico (TESTA)”, *DA, Revista de Documentación Administrativa* n° 284-285, mayo-diciembre 2009, Instituto Nacional de Administración Pública, Madrid, p. 50.

<sup>23</sup> ORTEGA CARBALLO C. (2006), “Los Registros administrativos como instrumentos de publicidad y transparencia en la gestión de la contratación pública”, *Documentación Administrativa / núm. 274-275 (enero-agosto 2006)*, Instituto Nacional de Administración Pública, Madrid, p. 108.

Teniendo en cuenta el conjunto de criterios y que la ponderación de los distintos casos se debe realizar atendiendo a los criterios de la normativa sobre protección de datos, y también de la normativa sobre transparencia administrativa, la dispersión de estos criterios en ambas normas no favorece a la necesaria seguridad jurídica, por lo que pueden realizarse mejoras normativas en el sentido de perfilar, en la regulación sobre transparencia administrativa, los principios que sirven para configurar la gestión y protección de datos en su normativa específica.

Se ha destacado también que los criterios introducidos por la normativa sobre protección de datos han superado a los criterios que dimanaban de la Ley de Transparencia, que debería ser revisada, ya que a pesar de haber ofrecido criterios para compatibilizar dos derechos destinados a entrar en conflicto en un momento inicial, adolece de algunos defectos que se han acentuado tras la entrada en vigor de la regulación actual sobre protección de datos<sup>24</sup>.

Además, teniendo en cuenta que la digitalización favorece la globalización del tratamiento de datos, esta cuestión debe ser resuelta en la normativa aplicable. Ya encontramos un avance en este sentido, en la reciente Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público, pero la digitalización permite un efecto globalizado del tratamiento de datos, consecuencia de la globalización de las comunicaciones<sup>25</sup>, siendo necesario aproximar su regulación en sistemas normativos con diferente tradición jurídica - *Continental Law* frente al *Common Law*-, puesto que las diferencias estructurales dejan de tener sentido en un sistema que acoge relaciones globalizadas<sup>26</sup>.

---

<sup>24</sup> RAMS RAMOS L. (2018), “El Derecho Fundamental a la protección de datos de carácter personal como límite ¿(in)franqueable? Para la transparencia administrativa, *Estudios de Deusto* 66, nº 2, p.150.

<sup>25</sup> CERVERA NAVAS L. (2003), “El modelo europeo de protección de datos de carácter personal”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, p. 132.

<sup>26</sup> MANNY C. (2003), “La intimidad de la Unión Europea y la seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de los Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, p. 146.

## 5. CONCLUSIONES

La protección de los datos personales entra en conflicto con el cumplimiento de las obligaciones de transparencia administrativa, especialmente, con el derecho de los ciudadanos al acceso a los expedientes tramitados por las Administraciones, ya que en ellos, se dan un sinfín de situaciones en las que los datos tratados son de diferente naturaleza, lo que conlleva una ponderación de la posibilidad de comunicar y difundir esos datos de forma casuística.

La ponderación, en estos casos, no es una tarea fácil debido a la especial cualificación de ambos derechos, pues ambos son Derechos Fundamentales, conectados directa o indirectamente con los Derechos Humanos, según la tesis que se acoja sobre la identidad entre Derechos Fundamentales y los Derechos Humanos.

Para realizar esta ponderación, tanto la regulación de la transparencia administrativa, como la de protección de datos personales, prevén ciertos criterios para preservar los datos más sensibles y para orientar la aplicación práctica de las reglas sobre protección de datos, permitiendo, en ciertos casos, la prevalencia de la transparencia administrativa.

La normativa sobre protección de datos tiene una importante base en el Derecho de la Unión Europea y cuenta con regulación especial en España, y la transparencia administrativa se encuentra básicamente regulada en normativa estatal o autonómica, pero interna, que es anterior a la regulación sobre protección de datos, y que adolece de algunos defectos que deberían ser solucionados a la luz de la regulación actual sobre protección de datos de carácter personal. En ambas, sin embargo, no se prevé cómo controlar la protección de datos a escala internacional, a pesar de que, como se ha indicado, los criterios para proteger datos personales deben ser aplicados al tratamiento posterior de los datos obtenidos a través del ejercicio del derecho de acceso, por lo que sería aconsejable que, dado que la digitalización permite una mayor difusión y comunicación de datos, hubiera una previsión de su protección a escala global, respecto de la que la reciente Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público, es un primer paso.

Debido a las dificultades para llevar a cabo la ponderación casuística de los derechos en conflicto, una acción que sí serviría para mejorar la posición del ciudadano en aras a conseguir una mejor protección de sus datos personales es formar e informar al

ciudadano de sus derechos en este ámbito, y de los mecanismos para reclamar el respeto a sus derechos, por lo que la normativa sobre protección de datos debería incluir un mandato dirigido a los poderes públicos para impulsar la formación del ciudadano en este ámbito.

## REFERENCIAS

ACED FÉLEZ, E. (2008). *Protección de Datos y e-Administración*. Agencia de Protección de Datos de la Comunidad de Madrid, Madrid, pp.1-11.

AGUILAR CAVALLLO, G. (2010). “Derechos Fundamentales-Derechos Humanos. ¿Una distinción válida en el siglo XXI?”, *Boletín Mexicano de Derecho Comparado*, número 127, pp. 15-71.

ARENA, G. (1997). “La transparencia administrativa”, *Documentación Administrativa*, nº 248-249 (mayo-diciembre 1997), Instituto Nacional de Administración Pública, Madrid, pp. 361 – 405.

ÁVILA RODRÍGUEZ, C.M. (2009). “El derecho ciudadano a una Buena Administración”, En Gutiérrez Rodríguez F.J. (Dir.), *El derecho de la ciudadanía a una Buena Administración. La Administración Electrónica*. Málaga: Diputación de Málaga.

CALVO ROJAS, E. (2003). “Algunas consideraciones sobre el procedimiento sancionador en el ámbito de la protección de datos personales”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, pp. 215 – 230.

CAZURRO BARAHONA, V. (2008). “La protección de datos y los medios de comunicación”, *Revista Jurídica de Castilla y León*, n.º 16, septiembre 2008, Junta de Castilla y León, León, pp. 227-256.

CERVERA NAVAS, L. (2003). “El modelo europeo de protección de datos de carácter personal”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, pp. 131 - 143.

- FERNÁNDEZ RAMOS, S. (2017). “Acceso a la información pública versus protección de datos personales”, *Revista española de Derecho Administrativo*, núm. 184.
- GAMERO CASADO, E. (2009). “El régimen de notificaciones: la dirección electrónica vial (DEV) y el tablón edictal de sanciones de tráfico (TESTA)”, *DA, Revista de Documentación Administrativa*, nº 284-285, mayo-diciembre 2009, Instituto Nacional de Administración Pública, Madrid, pp. 33-60.
- GIMENO FELIU, J.M. (2017). “La transposición de las directivas de contratación pública en España: una primera valoración de sus principales novedades”, *Documentación Administrativa, Nueva Época – Nº 4*, Enero-Diciembre 2017, Instituto Nacional de Administración Pública, Madrid, pp. 7-30.
- GUASCH PORTAS, V. y SOLER FUENSANTA, J.R. (2015). “El interés legítimo en la protección de datos”, *Revista de Derecho UNED*, núm. 16, Universidad Nacional de Estudios a Distancia, Madrid, pp. 417 - 438.
- GUICHOT, E. (2007). “Acceso a la información en poder de la Administración y protección de datos personales”, *Revista de Administración Pública*, núm. 173, Ed. Instituto Nacional de Administración Pública, Madrid.
- JEGOUZO, I. (1994). “El derecho a la transparencia administrativa: el acceso de los administrados a los documentos administrativos”, *Documentación Administrativa / nº 239* (julio-septiembre 1994), Instituto Nacional de Administración Pública, Madrid, pp. 11 – 29.
- MANNY, C. (2003). “La intimidad de la Unión Europea y la seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de los Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, pp. 145 – 177.
- MARTÍN-RETORTILLO BAQUER, L. (2006). *Vías concurrentes para la protección de los derechos humanos*. Navarra: Thomson Reuters-Civitas.

- MEILÁN GIL, J.L. (2013). “La buena administración como institución jurídica”, en *Revista Andaluza de Administración Pública*, núm. 87, Sevilla, pp. 13-50.
- ORTEGA CARBALLO, C. (2006). “Los Registros administrativos como instrumentos de publicidad y transparencia en la gestión de la contratación pública”, *Documentación Administrativa* / núm. 274-275 (enero-agosto 2006), Instituto Nacional de Administración Pública, Madrid, pp. 93 – 113.
- PIÑAR MAÑAS, J.L. (2003). “El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, pp. 45 - 90.
- PIÑAR MAÑAS, J.L. (dir.) (2014). *Transparencia, acceso a la información y protección de datos*, Ed. Reus.
- RAMS RAMOS, L. (2018). “El Derecho Fundamental a la protección de datos de carácter personal como límite ¿(in)franqueable? Para la transparencia administrativa”, *Estudios de Deusto* 66, nº 2, pp. 119-152.
- RIBAGORDA GARNACHO, A. (2008). “La protección de datos personales y la seguridad de la información”, *Revista Jurídica de Castilla y León*, n.º 16, septiembre 2008, Junta de Castilla y León, León, pp.373-399.
- RODOTÀ, S. (2003). “Democracia y protección de datos”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, pp. 15-26.
- RODRIGUEZ ÁLVAREZ, J.L. (2016). “Transparencia y protección de datos personales: criterios legales de conciliación”, En Canals Ametller (ed.), *Datos, Protección, Transparencia y Buena Regulación*, Ed. Documenta.
- SPANISH PERSONAL DATA AGENCY (2018). *Report answering the consultation about compliance of Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016*, Personal Data Agency, Spain, pp. 1-23.

TOMÁS MALLÉN, B. (2004). *El derecho fundamental a una buena administración*, Madrid: editado por Instituto Nacional de Administración Pública.

TRONCOSO REIGADA, A. (2003). “La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional”, *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003), Instituto Nacional de Administración Pública, Madrid, pp. 232–334.