

## **DERECHO A LA PRIVACIDAD, TRANSPARENCIA Y EFICACIA ADMINISTRATIVA: UN DIFÍCIL Y NECESARIO EQUILIBRIO**

Emilio Guichot Reina\*

### **Sumario**

- I. Introducción
- II. La tensión entre el derecho a la protección de datos y la eficacia administrativa
- III. La tensión entre el derecho a la protección de datos y el acceso a la información pública

---

\* Emilio Guichot Reina, profesor titular de derecho administrativo de la Universidad de Sevilla, Facultad de Derecho, Avda. del Cid, s/n, 41004 Sevilla, [eguichot@us.es](mailto:eguichot@us.es).  
Artículo recibido el 14.07.2007.

## I. Introducción

Analizamos en este trabajo la tensión entre el derecho a la protección de datos y los principios de eficacia y transparencia administrativa. Se trata de un tema crucial del derecho público de la información necesitado de una profunda reflexión que en nuestro derecho está aún por hacer. En este artículo se formulan claves generales que pretenden contribuir modestamente al necesario esclarecimiento de la cuestión.<sup>1</sup>

## II. La tensión entre el derecho a la protección de datos y la eficacia administrativa

El flujo informativo de información que contenga datos personales dentro de una misma Administración pública y entre administraciones públicas diferentes no plantea mayor problemática jurídica cuando tiene lugar previo consentimiento informado del interesado. Es más, resulta de gran interés apuntar la existencia de normas que en los últimos años han ido configurando el derecho de los ciudadanos a no aportar documentación que obre en poder de la misma e incluso de distinta Administración.

El artículo 35.f de la Ley 30/1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, de 26 de noviembre (en adelante, LRJAP-PAC), reconoce el derecho de los ciudadanos en sus relaciones con las administraciones públicas a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate, o que ya se encuentren en poder de la Administración actuante.<sup>2</sup> Se trata de un derecho del ciudadano –que puede acogerse o no al mismo, pues requiere su con-

---

1. Sobre el derecho a la protección de datos frente a la Administración pública, en general, nos remitimos a nuestra monografía *Datos personales y Administración Pública*, Civitas, 2005, y al artículo «Derecho a la protección de datos y actividad administrativa», *Revista Vasca de Administración Pública*, núm. 71, 2005, pp. 81-120.

2. Este derecho ha sido objeto de desarrollo para las actuaciones ante la Administración del Estado por el Real decreto 1778/1994, de 5 de agosto, que adecua las normas reguladoras de los procedimientos administrativos para el otorgamiento, modificación y extinción de autorizaciones; en su artículo 2, denominado «aportación de documentos», precisa que el ejercicio de este derecho tiene como condición que el ciudadano haga constar la fecha y el órgano o dependencia en que fueron presentados o, en su caso, emitidos, y que no hayan transcurrido más de cinco años des-

sentimiento— y es operativo sólo en el seno de una misma Administración pública, no respecto a documentos obrantes en poder de una Administración pública diversa a aquélla que tramita el procedimiento. Desde el punto de vista del derecho a la protección de datos, no hay objeción alguna que hacer, puesto que el principio del consentimiento resulta crucial a estos efectos: el derecho a la protección de datos es un derecho que trata de garantizar, no la reserva absoluta de los mismos, sino, precisamente, las facultades de disposición y control de los ciudadanos sobre sus datos, esto es, la «autodeterminación informativa», como se ha llamado al propio derecho. Lo que explica que, conforme a los artículos 6, 7 y 11 de la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante, LOPD), con el consentimiento de los interesados los datos puedan ser tratados y comunicados, respetando, claro está, el resto de principios y derechos que conforman el contenido del derecho a la protección de datos.

Resulta de la mayor actualidad e interés reseñar que la recentísima Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios

---

de la finalización del procedimiento a que correspondan. Además, que en los supuestos de imposibilidad material de obtener el documento, debidamente justificada en el expediente, el órgano competente podrá requerir al solicitante su presentación o, en su defecto, la acreditación por otros medios de los requisitos a que se refiere el documento, con anterioridad a la formulación de la propuesta de resolución. Condiciones, todas ellas, que se recogen asimismo en la normativa sobre subvenciones. Así se regula la cuestión en los art. 23.3 de la Ley 38/2003, de 17 de noviembre, general de subvenciones, y 4.2 del Real decreto 225/1993, de 17 de diciembre, que aprueba el reglamento de procedimiento para concesión de las subvenciones públicas; si bien ambos reproducen esta previsión, no tienen carácter básico. En aplicación del artículo 35.f de la LRJAP-PAC se aprobaron el año pasado los reales decretos 932 y 933/2006, de 28 de abril, que suprimen, respectivamente, la aportación de fotocopias de documentos de identidad y del certificado de empadronamiento como documento probatorio del domicilio y la residencia, en los procedimientos administrativos de la Administración general del Estado y de sus organismos públicos vinculados o dependientes. En estos casos, la comprobación de los datos se hace de oficio por el órgano instructor, de acuerdo con los datos de identificación que obren en sus archivos, bases de datos u otros fondos documentales, o, cuando sea imprescindible la acreditación fehaciente, mediante un sistema informático de Verificación de Datos de Identidad, cuyo responsable es la Dirección General de la Policía y de la Guardia Civil (desarrollado por Orden PRE/3949/2006, de 26 de diciembre), y de Verificación de Datos de Residencia, cuyo responsable es el Instituto Nacional de Estadística (desarrollado por Orden PRE/4008/2006, de 27 de diciembre). En este caso se requiere consentimiento del interesado, que debe constar en la solicitud de iniciación del procedimiento o en su recibo de presentación, o en cualquier otra comunicación posterior. Caso de no prestar su consentimiento, deberá aportar fotocopia del documento de identidad.

públicos, ha regulado, en sus artículos 6.2.<sup>b3</sup> y 9,<sup>4</sup> el derecho de los ciudadanos a no aportar datos y documentos que obren en poder de otras administraciones públicas y las transmisiones de datos entre administraciones públicas a que el ejercicio de dicho derecho da origen. Se trata de una modalización del derecho reconocido en el artículo 35.f para los casos de tramitación electrónica de procedimientos, pero supone una ampliación del contenido de éste, ya que no se limitan a posibilitar el ejercicio del derecho a no aportar los datos y documentos que obren en poder de la Administración que tramita el procedimiento, sino de cualquier Administración pública. En estos casos, se requiere el consentimiento del interesado –en la forma que estipula la LOPD y su futuro reglamento de desarrollo, y que diverge, como es sabido, en función de que se trate o no de datos especialmente protegidos– cuando contengan datos personales (de lo contrario, habrá de aportarlos él mismo, ha de entenderse), consentimiento que obliga a la Administración actuante a recabarlo por vía electrónica del órgano de la misma o distinta Administración en cuyo poder se encuentren y a ésta última a comunicarlos a la primera, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. Pero junto a este «derecho», entendido como posibilidad de no aportar documentación que contenga datos personales, consintiendo que la Administración que tramite la requiera directamente a la que lo detenta, la ley ha contemplado la posibilidad de prescindir de dicho consentimiento, en los casos en que las diversas disposiciones legales así lo permiten, posibilidad que, como veremos a continuación, se

---

3. «A no aportar los datos y documentos que obren en poder de las administraciones públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley orgánica 15/1999, de protección de datos de carácter personal, o una norma con rango de ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.»

4. «1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b, cada Administración deberá facilitar el acceso de las restantes administraciones públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su normativa de desarrollo. 2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b de la presente Ley.»

contempla en muy diversos sectores de la actividad administrativa, con independencia de que la solicitud de información se tramite o no en el marco de un procedimiento electrónico. En ambos casos, si los datos se encuentran en soporte electrónico, se prevé la interconexión que la Ley parece convertir en una obligación en las relaciones interadministrativas. Todo ello se compatibiliza expresamente en la Ley con respeto al principio de adecuación, de finalidad y de seguridad, y, en general, a la normativa sobre protección de datos, por lo que, a nuestro juicio, esta Ley se acompasa bien con la misma, y no merece reproches desde la óptica de ese derecho.<sup>5</sup>

En conexión con lo que acabamos de señalar, es preciso ahora plantearse si, en efecto, en determinados casos puede existir el deber de un órgano administrativo de poner a disposición de cualquier órgano administrativo de la misma o de distinta Administración la información personal que detente un documento cuando se le requiera para el ejercicio por aquéllos de sus competencias. Esto es, no se trataría ya de flujos informativos que presuponen el consentimiento del ciudadano, sino que operan al margen del mismo. No hablaríamos ya del ejercicio de un derecho del ciudadano, sino de una facultad de un órgano administrativo de recabar información de otro al que se le impone el deber de dar cumplimiento a dicho requerimiento. Dicho flujo incontestado es pensable tanto dentro de una misma Administración como entre administraciones públicas.

Desde la perspectiva de la LOPD, el consentimiento para el *tratamiento de datos dentro de una misma Administración* (en sentido estricto, esto es, su utilización por la Administración que los posee) no es necesario cuando los datos se recogen para el ejercicio de las funciones propias de las administraciones públi-

---

5. Por lo demás, no es del todo nuevo bajo el sol ya que el precepto no sólo entronca con el artículo 35.f de la LRJAP-PAC, sino también con otras previsiones aplicables hasta ahora tan sólo en el ámbito de la Administración estatal, como la innecesariedad de adjuntar fotocopias de documentos identificativos y certificados de empadronamiento, a la que hicimos ya alusión, o lo dispuesto en el Real decreto 209/2003, de 21 de febrero, que regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, que introdujo un nuevo capítulo V en el Real decreto 263/1996, de 16 de febrero, titulado «Certificados telemáticos y transmisiones de datos». Dicho Real decreto previó la sustitución de certificados en soporte papel por certificados telemáticos o por transmisiones de datos, y reguló ambas figuras, condicionando su utilización en ambos casos al consentimiento del interesado o a la existencia de una previsión legal que lo autorice y especificando que la expedición, tratamiento y efectos se rigen por la LOPD.

cas en el ámbito de sus competencias.<sup>6</sup> La Ley no regula de forma expresa la comunicación de datos de un órgano administrativo responsable de un fichero a otro de la misma Administración. A falta de una clarificación, y conforme a una interpretación coherente y sistemática de la Ley, ha de entenderse que ésta cabe siempre que se respete el principio de finalidad, en el entendimiento que éste haya de tener, y que como se sabe, y aunque parezca mentira, es discutido. Y es que la LOPD no impone la utilización de los datos para la finalidad para la que fueron recabados, sino que, de forma negativa, la proscribire para *finalidades incompatibles*, precisando a continuación que no se considera como tal el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.<sup>7</sup> En esto se separa de su predecesora, la Ley orgánica 15/1999, de 13 diciembre, de protección de datos de carácter personal (en adelante, LORTAD), que prohibía todo uso para una *finalidad distinta* de aquella para la que los datos hubieran sido recogidos.<sup>8</sup> Ciertamente, que sea un fin incompatible con otro resulta har-to difícil de determinar. La trascendencia de este cambio de redacción es aún objeto de debate en la doctrina, la jurisprudencia y las agencias estatal y autonómicas de protección de datos.<sup>9</sup> A nuestro juicio, hay que convenir que se trata de una expresión desafortunada, puesto que, de lo contrario, el precepto chirr-ría con todo el sistema de la Ley, basado precisamente en el principio de la afectación de los datos a finalidades concretas y predeterminadas. En este pun-

---

6. Art. 6.2 LOPD.

7. Art. 4.2 LOPD.

8. Art. 4.2 LORTAD. La interpretación de la Agencia de Protección de Datos española era además estricta. Por poner una muestra, en la Memoria 1998 venía a considerarse que la utilización de datos de jóvenes, obtenidos para el reclutamiento, al objeto de dirigirles información sobre la campaña del Ministerio de Defensa para la captación de tropa profesional suponía una desviación de la finalidad inicial prohibida por la LORTAD.

9. La Sentencia de la Audiencia Nacional de 11 de febrero de 2004 afirma que el término «incompatibles» del artículo 4 de la LOPD debe ser interpretado sistemáticamente y no literalmente, lo que en la práctica significa seguir apegado al concepto de finalidad distinta, criterio éste que sigue, por ejemplo, la Agencia de Protección de Datos de la Comunidad de Madrid. Hasta la aprobación de la LOPD, la Agencia de Protección de Datos partía de este entendimiento del principio de finalidad. A partir de esa fecha entiende, de una parte, que la LOPD ha supuesto un reforzamiento del principio, en la medida en que se exige la precisión inicial de fines «determinados y explícitos» (Memoria de 1999). Pero, por otra, se ha hecho eco del cambio en la redacción, y considera que «[...] (d)ado que la Ley no identifica qué ha de entenderse por “fin compatible”, debe analizarse la existencia de dicha compatibilidad en cada supuesto de hecho que se plantee, determinando si a la luz de las disposiciones aplicables a cada caso y de las circunstancias del mismo cabe considerar que esa finalidad que se alega como compatible resulta lícita a la luz de las normas aplicables y si la misma guarda una adecuada relación con la finalidad que justificó el tratamiento de los datos».

to, la confrontación con la normativa europea y comparada resulta de especial utilidad, ya que la Ley reproduce, de forma no literal, lo previsto en la normativa europea, que lo que prohíbe es la *utilización o tratamiento incompatible* con la finalidad para la que los datos fueron recabados.<sup>10</sup> La expresión no tendría, pues, más virtualidad que la de dar cabida a su excepción, que es única y precisamente la contemplada en el propio apartado, según el cual «no se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos», y ello en atención a la ausencia general de riesgo para los derechos de la persona que se deriva de este género de tratamientos. Se echa en falta, en todo caso, una clarificación de un punto absolutamente crucial y que afecta a todo el sistema.<sup>11</sup>

Respecto a las comunicaciones de datos entre administraciones públicas distintas, pueden llevarse a cabo con el consentimiento del afectado o sin éste, cuando los datos hayan sido obtenidos o elaborados por una Administración con destino a otra, o tenga lugar para el ejercicio de las mismas competencias o de competencias que versen sobre las mismas materias.<sup>12</sup> El primero de estos supuestos se caracteriza por la instrumentalidad en la actividad de la Administración cedente. En estos casos, y conforme a las definiciones legales, habría de entenderse que no se produce en realidad una cesión, en la medida en que la Administración cedente actúa como encargada del tratamiento, y la cesionaria es la auténtica responsable del fichero o tratamiento. En él se encuadran los casos de colaboración interadministrativa, articulada a menudo como encomienda de gestión o como delegación de competencias. Un supuesto destacado sería la elaboración por las diputaciones de los padrones de pequeños municipios. También los casos de presentación de escritos en registros de una Administración con destino a otra, acogidos en el art. 38.4 Ley 30/1992. Por su parte, el ré-

---

10. Conforme al Convenio 108 (artículo 5.b): «Los datos de carácter personal que sean objeto de un tratamiento automatizado se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades». De acuerdo con la Directiva de 1995 (artículo 6.1.b): los datos personales serán «recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los estados miembros establezcan las garantías oportunas».

11. El Grupo Parlamentario Socialista presentó una Proposición de Ley orgánica de modificación de la LOPD de reforma del artículo 4.2 para sustituir la nueva referencia a las finalidades «incompatibles» y volver a la anterior de finalidades «distintas» (BOCG, serie B, núm. 233-1, de 26 de abril de 2002).

12. Art. 21 LOPD.

gimen general de la comunicación interadministrativa se caracteriza por una absoluta oscuridad, que trae su causa tanto del dictado de la Ley, que utiliza una formulación en negativo y unos conceptos de difícil encaje en la sistemática legal, como en que la redacción inicial del precepto ha quedado alterada tras la declaración de inconstitucional llevada a cabo por la STC 292/2000.<sup>13</sup> Conforme a esta jurisprudencia constitucional, habría que distinguir, pues, dos supuestos:

a) Cuando la comunicación de datos tiene como destino su empleo por otra Administración para la misma finalidad para la que han sido recabados y tratados, no se precisa el consentimiento del interesado, si bien la comunicación ha de preverse en la disposición de creación del fichero.<sup>14</sup> En este caso, no se requiere consentimiento del afectado (como no lo requiere la normativa europea), y la explicación sería que la efectividad de los fines públicos, que han legitimado previamente la obtención de los datos, requiere que el reparto territorial de competencias no sea óbice para su efectividad y para una actuación coordinada entre los órganos de las diversas administraciones con competencia sobre la materia.

b) Cuando la comunicación de datos tiene como destino su empleo por otra Administración para una finalidad distinta de aquélla para la que han sido recabados y tratados, conforme al dictado de la STC 292/2000, es preciso una previsión legal expresa, en cuyo caso puede llevarse a cabo sin consentimiento

---

13. El precepto disponía que: «Los datos de carácter personal recogidos o elaborados por las administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos». Esta dicción abría la posibilidad de previsión reglamentaria de comunicación de datos para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas (que podía llevarse a cabo en la propia disposición de creación del fichero), de modo que lo resaltado en cursiva fue considerado inconstitucional en la STC 292/2000.

14. Hacemos referencia al principio de finalidad, siendo así que el art. 21 alude al criterio de las «competencias diferentes» y las «competencias que versen sobre materias distintas». Los términos utilizados conllevan una gran dificultad hermenéutica y han dado lugar a interpretaciones doctrinales muy diversas. Entendemos que la Ley ha querido asegurar la libre circulación de datos entre administraciones siempre que se mantenga una identidad de destino, lo que vendría a coincidir con el concepto de «materia» (medio ambiente, seguridad, tributos, etc.).

del afectado. El análisis de la normativa sectorial muestra que las leyes especiales que autorizan la comunicación de datos incoherente intra o interadministrativas, discriminando supuestos en que cabe y otros en que no, lo hacen atendiendo a criterios carentes de motivación y de elementos ponderativos, a menudo del modo más amplio la cesión interadministrativa de datos personales sin consentimiento en sectores clave de la actividad administrativa, como Hacienda o la Seguridad Social, y declaran inaplicable el régimen de la comunicación de datos diseñado en el art. 21.1 LOPD (a efectos de eliminar la limitación de la identidad de finalidades).<sup>15</sup> Además, ha de tenerse en cuenta que los datos esenciales de las personas (nombre, apellidos, domicilio, sexo, fecha y lugar de nacimiento, DNI, nivel de estudios) están a disposición de todas las administraciones públicas para el ejercicio de sus respectivas competencias, a través del padrón municipal y el fichero o registro de población creado por la LOPD.<sup>16</sup> Lo mismo cabe decir de los datos catastrales, también los reservados, que se consideran a disposición de todas las administraciones «con las limitaciones derivadas de los principios de competencia, idoneidad y proporcionalidad».<sup>17</sup>

---

15. Así, p. ej., en materia tributaria (art. 93 a 95 Ley 58/2003, de 17 de diciembre, general tributaria, desarrollados por Orden del Ministerio de Economía y Hacienda de 18 de noviembre de 1999, que regula el suministro de información tributaria a las administraciones públicas para el desarrollo de sus funciones); o de recaudación de derechos de la Seguridad Social (art. 36 Real decreto legislativo 1/1994, de 20 de junio, por el que se aprueba el texto refundido de la Ley general de la Seguridad Social).

16. En efecto, por una parte, la normativa reguladora del padrón municipal (en el que los ciudadanos han obligatoriamente de inscribirse) prevé la cesión de datos del padrón a otras administraciones públicas como obligatoria para los ayuntamientos y no requiere el consentimiento previo, si bien debe limitarse a aquellos casos en que sea necesario *para el ejercicio de sus respectivas competencias*, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. Dichos datos son muy relevantes (nombre, apellidos, domicilio, sexo y fecha y lugar de nacimiento, DNI –o equivalente para extranjeros– y el nivel de estudios –art. 16 y 17 LRBRL). Por su parte, sobre la base del padrón y del censo electoral que se forma a partir del mismo la LOPD ha establecido la creación de los llamados ficheros o registros de población, previendo su cesión interadministrativa incoherente para *cualquier finalidad que se encuentre dentro del ámbito competencial de cada Administración* (disposición adicional segunda: «1. La Administración general del Estado y las administraciones de las comunidades autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. 2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las administraciones públicas»).

17. Art. 51 a 53 Real decreto legislativo 1/2004, de 5 de marzo.

O de los datos del Registro de la propiedad, cuya comunicación se prevé, genéricamente, a instancias de cualquier autoridad administrativa.<sup>18</sup> De esta suerte, podría decirse que a la postre las administraciones se comunican con práctica libertad los datos personales de los ciudadanos que les son necesarios para el ejercicio de sus competencias, sin el consentimiento de los interesados. Como único contenido auténticamente garantizado está que toda comunicación se supedita a la necesidad y adecuación de los datos para el desempeño de sus funciones en la materia específica sobre la que cada Administración, y dentro de ella, cada órgano, es competente. Es más, en muchos casos se prevén conexiones directas a bases de datos donde figuran datos personales, como en el caso de los datos de extranjeros que figuran en el padrón municipal, el Registro de la propiedad, las bases de datos de Hacienda, entre otros.<sup>19</sup> En efecto, cada vez son más las previsiones normativas que posibilitan el acceso a bases de datos personales a un sujeto distinto del responsable y que no se halla bajo su dependencia, sin la intermediación de dicho responsable. A falta de una regulación específi-

---

18. Art. 332.6 Reglamento hipotecario.

19. En este sentido, puede citarse la Orden del Ministerio de Economía y Hacienda de 18 de noviembre de 1999, que regula el suministro de información tributaria a las administraciones públicas para el desarrollo de sus funciones, con consentimiento del interesado pero también sin él, en los casos previstos en la Ley general tributaria. En ambos casos, tiene como posibles destinatarias a las distintas administraciones públicas. El artículo 5 regula el acceso mediante consulta a bases de datos tributarias en los supuestos previstos antes en el artículo 113.1 de la anterior Ley general tributaria y hoy en el artículo 95.1 de la vigente, por los sujetos contemplados en dicho artículo, en casos excepcionales, y en condiciones de seguridad, constancia de la identidad del consultante y la finalidad de la consulta, etc. Más amplia es la posibilidad que brinda la legislación hipotecaria, tras la reforma por Ley 24/2005, de 18 de noviembre, que permite el acceso directo por vía telemática al contenido de los libros registrales de todas las autoridades, empleados o funcionarios públicos que actúen por razón de su oficio o cargo, a quienes la Ley hipotecaria presume el interés en averiguar el estado de los bienes inmuebles o derechos reales inscritos. De todos, el mecanismo más polémico se encuentra en la normativa del padrón. En efecto, la Ley orgánica 14/2003, de 20 de noviembre, introdujo una disposición adicional quinta en la Ley orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, que prevé que los órganos administrativos competentes en materia de extranjería tengan «acceso directo» a los ficheros de la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística—este último en lo relativo al Padrón Municipal de Habitantes— en los que obren datos que hayan de constar en los expedientes que tramitan, sin necesidad de consentimiento del interesado, y asimismo, a estos efectos, se introdujo también en la Ley 7/1985, de 2 de abril, de bases del régimen local, una disposición adicional séptima, bajo el rótulo «acceso a los datos del padrón», que permite el acceso de la Dirección General de la Policía a los datos de extranjeros que figuren del padrón, «preferentemente por vía telemática», con medidas de seguridad que permitan la constancia de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados, para garantizar el derecho a la protección de datos. Estas previsiones han sido muy polémicas. La previsión de acceso de la Dirección General de la Policía a los datos de inscripción del padrón de los extranjeros, «preferentemente por vía telemática»,

ca, la conexión directa a bases de datos supone un reto de conceptualización, pues hay que decidir si el que accede tiene la consideración de usuario o de tercero al que se comunican datos. A nuestro juicio, una interpretación sistemática de la Ley aboga por reservar el concepto de usuario a las personas que se encuentran bajo el ámbito de dirección del responsable o responsables del fichero, entendiendo que en los demás casos se trata de una cesión. La propia LOPD incluye dentro del concepto de tratamiento cualquier operación, también «las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias». El problema radica en que este tipo de interconexión supone un riesgo de «descontrol» de la efectividad del derecho, en la medida en que los principios y facultades que lo integran pueden llegar a desvanecerse, ya que todo el sistema de la LOPD parte y presupone que es el responsable del fichero el que garantiza la vigencia de los principios de finalidad y de adecuación; el que posibilita el ejercicio de los derechos de oposición, acceso, rectificación y cancelación; el que responde de las medidas de seguridad y secreto, y el que responde ante el afectado (derecho a indemnización) y ante la Agencia de Protección de Datos (régimen sancionador) por los incumplimientos.<sup>20</sup>

---

para el ejercicio de sus competencias sobre control y permanencia de los extranjeros fue objeto de enmiendas por diputados del Grupo Mixto, del PNV y de IU, así como del PSOE, si bien éste último aceptó una enmienda transaccional que autoriza el acceso de la policía al padrón municipal pero con garantías no previstas en el proyecto original, relativas a las máximas medidas de seguridad, la constancia de los accesos, la identificación de usuario, fecha y hora del acceso y datos consultados a las que hemos hecho referencia. La Agencia de Protección de Datos española elaboró un informe específico sobre esta previsión normativa, el número 211/2004. No obstante, el mecanismo sigue siendo polémico, aparte el hecho de permitir el acceso directo telemático, por hacerlo para finalidades incompatibles con las que motivan la recogida, pues se considera —a nuestro juicio, razonablemente— que existe una contradicción entre fomentar la inscripción padronal como modo de integración social y de acceso a servicios públicos, y utilizar esa información con fines de control policial y, en su caso, de expulsión. Ello explica que haya dado origen al planteamiento de un recurso de inconstitucionalidad (recurso de inconstitucionalidad núm. 1024-2004, promovido por el Parlamento vasco). En todo caso, la posibilidad de acceso telemático se produce sólo por parte de un órgano administrativo concreto (la Dirección General de la Policía), sólo a determinados datos que el propio sistema informático depura, y para una finalidad determinada y pública.

20. La escasa y cualificada doctrina que se ha ocupado de la cuestión ha puesto de relieve la potencial contradicción entre la eficacia que proporciona el intercambio telemático de información y el derecho a la protección de datos personales (Valero Torrijos, J. y Fernández Salmerón, M., *La protección de los datos personales y las Administraciones Públicas en la Unión Europea* (en prensa). Reflexión que profundiza en la línea trazada por el Documento de trabajo sobre la Administración en línea, de 8 de mayo de 2003, del Grupo de trabajo sobre protección de datos del artículo 29 de la Directiva 95/46/CE (este Grupo de trabajo es un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sitio web: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)).

En estos casos, resulta evidente la necesidad de configurar la conexión de manera tal que garantice el cumplimiento de la normativa sobre protección de datos (en especial, acceso por personas identificadas, para fines determinados permitidos legalmente, a los datos estrictamente necesarios para los mismos, y con seguridad en la comunicación telemática), lo que puede desactivar los peligros apuntados.

Ahora bien, dicho esto, en lo que se refiere a la necesidad de consentimiento o de previsión legal expresa para la comunicación de datos, cuando se pretendan destinar a una finalidad distinta a la que motivó la recogida, nos parece posible argumentar que, frente a la actividad administrativa, ningún riesgo corre el ciudadano por el hecho de que sus datos personales sean trasladados libremente en el interior de una misma Administración o de una Administración a otra para el ejercicio de las competencias respectivas por cada órgano dentro de cada Administración en sus diversos ámbitos competenciales. Aunque podría tratarse de una afirmación aparentemente herética,<sup>21</sup> entendemos que el control frente a los posibles abusos radicaría, precisamente, en la combinación de los principios de legalidad de la actuación administrativa y calidad de los datos, que impediría a cualquier órgano administrativo acumular más datos de los estrictamente necesarios para el cumplimiento de sus funciones. Cualquier desviación sería contraria a estos principios, y, por ende, ilegal, mientras que el ciudadano no debería sentir amenaza alguna por el correcto ejercicio de sus competencias por parte de las administraciones a partir de datos personales veraces, y conservaría en todo caso sus facultades de información, acceso, rectificación y cancelación para controlar el cumplimiento de estos presupuestos. De este modo, el principio de eficacia administrativa (que, dependiendo del sector, puede ponerse en relación con el derecho a la salud, a la seguridad, al sostenimiento equitativo de las cargas públicas, etc.) unido, en el caso de las cesiones interadministrativas, al deber de cooperación hoy expresado en el art. 4 LRJAP-PAC, pugnaría por un flujo sin limitaciones de datos entre administraciones públicas para el ejercicio de sus respectivas competen-

---

21. Si bien parece apuntar también este sentido, A. Troncoso Reigada (en su prólogo al libro de Fernández Salmerón, M., *La protección de los datos personales en las Administraciones Públicas*, Civitas, Madrid, 2003) defiende que «impedir a una Administración pública utilizar ese fichero para una finalidad parcialmente distinta no tiene en ocasiones sentido al tener ésta la facultad de tratar datos personales sin consentimiento del interesado. La solución de pedirle el consentimiento sería contradictoria con el art. 6.2 LOPD» (p. 39, nota 41).

cias.<sup>22</sup> A fin de cuentas, el único límite añadido por el TC consiste en someter este libre tráfico a los requisitos generales de toda limitación a un derecho fundamental, lo que en la práctica viene a significar, fundamental y casi exclusivamente, someterlo a reserva de ley, reserva podría argumentarse si no puede considerarse cubierta por la obligación de colaboración interadministrativa prevista en el art. 4 LRJAP-PAC.<sup>23</sup> Ciertamente, puede argüirse que la declaración de inconstitucionalidad parcial del art. 21 LOPD llevada a cabo por la STC 292/2000 presupone una respuesta negativa, pero lo cierto es que otros preceptos de la misma LOPD tienen un alcance igualmente general y que una reserva de ley especial carece de la necesaria flexibilidad que puede exigir la colaboración administrativa en supuestos imprevistos (piénsese, por ejemplo, en una solicitud de información sobre los empresarios que fabrican determinado producto exigida a la Administración estatal tributaria por una Administración autonómica que la precisa para adoptar medidas sanitarias). Es más, debe tenerse en cuenta que, en ocasiones, en dichas disposiciones se prevé que un fichero cumpla más de una finalidad, integrándose cada una de ellas en el marco competencial de diferentes órganos administrativos. En este caso, el órgano responsable del fichero podrá ceder al que no lo sea los datos necesarios para alcanzar la finalidad prevista. El Tribunal Supremo ha entendido que la inconstitucionalidad de la previsión de la LOPD que permitía autorizar por reglamento la cesión de datos personales se refiere a la cesión para finalidad diferente a la contemplada en la norma de creación, y no para una de las finalidades ya ini-

---

22. En definitiva, ¿por qué no facilitar este trasvase de datos, cuando la Administración es una entidad de naturaleza vicarial al servicio de los intereses generales? ¿Acaso no originaría ello un mejor funcionamiento de las diferentes administraciones y un mejor reparto de las cargas públicas? (controlando, por ejemplo, que los ingresos consignados a efectos de solicitar una subvención coinciden con los declarados ante la Administración tributaria). ¿Qué interés digno de protección puede esgrimir el ciudadano para oponerse a este flujo informativo? No parece que haya en nuestro Estado democrático un riesgo cierto de acumulación silente de datos para formar perfiles individuales por parte de las administraciones públicas (lo cual, por lo demás, estaría abiertamente proscrito por los principios de legalidad y calidad).

23. En lo que hace a las relaciones interadministrativas, el artículo 4 de la LRJAP-PAC, en su apartado primero, establece, entre las manifestaciones del principio de lealtad institucional que rige las relaciones entre administraciones públicas, las siguientes: *c)* Facilitar a las otras administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias. *d)* Prestar, en el ámbito propio, la cooperación y asistencia activas que las otras administraciones pudieran recabar para el eficaz ejercicio de sus competencias. Y en su apartado segundo, dispone que: «A efectos de lo dispuesto en las letras *c* y *d* del apartado anterior, las administraciones públicas podrán solicitar cuantos datos, documentos o medios probatorios se hallen a disposición del ente al que se dirija la solicitud. Podrán también solicitar asistencia para la ejecución de sus competencias».

cialmente previstas. Sin embargo, lo cierto es que en todos los casos antes mencionados, en que se contemplan supuestos absolutamente generales de comunicación incontestada, el particular desconoce *de facto* cuáles serán los posibles destinos de sus datos, pese a que la normativa exige que las disposiciones reglamentarias de creación de cada fichero hagan constar las posibles cesiones, por lo que su previsión legal no se antoja una garantía de peso. Como argumento comparativo, ha de reseñarse que la autorización de cualquier comunicación intra e interadministrativa de datos para el ejercicio de las respectivas competencias está prevista en la propia normativa comunitaria que regula el tratamiento de datos por las instituciones, y puede derivarse de la Directiva de 1995, que no regula de forma específica la comunicación, sino que la integra dentro del concepto de tratamiento, y éste se legitima sin necesidad de consentimiento del interesado, siempre que es necesario para el cumplimiento de una misión pública o de una obligación legal. Creemos, pues, que el legislador español ha sido corto de miras y que el Tribunal Constitucional ha ido probablemente demasiado lejos en su aplicación mimética de la dogmática general de los límites de los derechos fundamentales. Como puede comprobarse, esta idea requiere una reflexión dogmática del mayor calado que vaya de la mano de una aproximación profunda (incluidos sus componentes extrajurídicos) acerca del entendimiento de cuál es la naturaleza de la relación Administración-ciudadanos.<sup>24</sup> Al respecto, no está de más recordar que los principios de eficacia y colaboración, como hemos apuntado, son principios constitucionales: el primero se encuentra recogido en el artículo 103.1 y sobre el segundo, el Tribunal Constitucional ha señalado –por todas, en su Sentencia 233/1999– que «no es menester justificar en preceptos concretos» y que «se encuentra implícito en la propia

---

24. Finalmente, lo dicho respecto a los datos personales «comunes» ha de complementarse con una reflexión acerca de la vigencia del principio de consentimiento en el caso de los datos especialmente protegidos. El art. 7 establece la prohibición absoluta de tratamiento de datos que revelen la ideología, afiliación sindical, religión y creencias sin consentimiento. Respecto a los relativos al origen racial, a la salud y a la vida sexual admite, además, que sean recabados, tratados y cedidos cuando por razones de interés general así lo disponga una ley. Este régimen se aplica aparentemente (la sistemática de la LOPD resulta realmente diabólica, y es útil acudir a la normativa comunitaria y comparada) tanto a los ficheros públicos como a los privados, en cuyo caso habría de concluirse que en estos supuestos es preciso que, o bien la propia LOPD, o bien una ley sectorial específica prevea el tratamiento (en sentido amplio) incontestado. Ello se hallaría en línea con la idea de que, al estar particularmente en juego en el manejo de estos datos la dignidad de la persona (con relación al principio de no discriminación y al derecho a la intimidad), toda posible afectación (bajo la forma de tratamiento incontestado) precisa de cobertura legal específica, justificada en la protección de un derecho o bien constitucional, sin que baste al respecto una mera norma reglamentaria general o la propia disposición de creación del fichero.

esencia de la forma de organización territorial del Estado que se implanta en la Constitución». Por tanto, con respeto de los límites y controles que el derecho establezca, ambos tienen también un papel determinante para el derecho administrativo, que no debe ser visto sólo como un derecho reactivo o de garantía.

### III. La tensión entre el derecho a la protección de datos y el derecho de acceso a la información pública

Como es sabido, el artículo 20 de la Constitución consagra la libertad de información y el 105 el derecho de acceso a la información en poder de la Administración. El desarrollo legal de este derecho se encuentra en los artículos 35.*n* y 37 de la LRJAP-PAC.<sup>25</sup>

Por su parte, el Tribunal Constitucional ha considerado que el artículo 18.4 supone el reconocimiento en nuestra Carta fundamental del derecho a la protección de datos;<sup>26</sup> tuvo su primer desarrollo legal en la LORTAD y actualmente se encuentra regulado en la LOPD y en sus reglamentos de desarrollo.

Reina el más absoluto silencio en ambos bloques normativos acerca de las relaciones entre acceso y protección de datos, silencio especialmente criticable cuando concurre la circunstancia de que la LORTAD y la LOPD son coetáneas, respectivamente, a la LRJAP-PAC y a su modificación por la Ley 4/1999, de 13 de enero.<sup>27</sup> El «olvido» legal de la necesidad de compatibilizar

25. Entre la doctrina que se ha ocupado del derecho de acceso en España, baste citar a Fernández Ramos, S., *El derecho de acceso a los documentos administrativos*, Marcial Pons, Madrid, 1997; Mestre Delgado, J. F., *El derecho de acceso a archivos y registros administrativos (Análisis del art. 105.b de la Constitución)*, Madrid, 1998; Parada Vázquez, R., *Régimen jurídico de las administraciones públicas y procedimiento administrativo común*, Marcial Pons, Madrid, 1999; Pomed Sánchez, L. A., «El acceso a los archivos administrativos: el marco jurídico y la práctica administrativa», *Revista de Administración Pública*, núm. 142, 1997; *El acceso de los ciudadanos a los archivos y registros administrativos*, INAP, Madrid, 1989; «La intimidad de las personas como límite al derecho de acceso a la documentación administrativa», en VA, *La protección jurídica del ciudadano. Libro homenaje al profesor González Pérez*, t. I, Civitas, Madrid, 1993; Villaverde Menéndez, I., *Los derechos del público*, Tecnos, Madrid, 1995.

26. Desde su Sentencia 254/1993, de 20 de julio.

27. Falta de la necesaria conexión ésta pese a la contemporaneidad en la aprobación de estas regulaciones que ha sido constatada por el propio Tribunal Supremo, en la STS de 31 de octubre de 2000, Ar. 9119 (ponente: González Navarro).

derechos e intereses se agudiza si tenemos en cuenta dos circunstancias. En primer lugar, que la LOPD, a diferencia de la Directiva comunitaria, no ha acogido la cláusula de la ponderación de derechos e intereses para el tratamiento in consentido; y que no ha establecido excepciones a la aplicación de la normativa sobre protección de datos respecto a los tratamientos con fines periodísticos, conectados directamente con la libertad de información del artículo 20 CE en contra de lo permitido por el artículo 9 de la Directiva de 1995 y lo previsto en la Recomendación 1/1997 del Consejo de Europa sobre la normativa respecto a protección de datos y los medios de comunicación.

La LRJAP-PAC parte de una distinción básica en el régimen aplicable entre los documentos que contengan datos íntimos, cuyo acceso está vedado de forma absoluta a terceros, a los que equipara el acceso a todo documento nominativo obrante en expedientes o ficheros de naturaleza sancionadora o disciplinaria. Como categoría intermedia entre los datos íntimos y los datos impersonales, la Ley se refiere a los documentos que contengan «datos nominativos» no íntimos, en cuyo caso se exige un interés directo para obtener el acceso. La LOPD, sencillamente, ignora la cuestión. Su artículo 11, que regula con carácter general el régimen de la comunicación de datos, no contempla específicamente este supuesto, que queda por tanto bajo el paraguas general que pueda otorgarle una ley que autorice la comunicación in consentida. Por su parte, el régimen específico de los ficheros públicos, que sí regula la comunicación de datos de una Administración pública a otra en el artículo 21, no contiene ninguna previsión respecto a su comunicación a particulares, salvo la relativa a la prohibición general de comunicación de datos recogidos de fuentes accesibles al público, que no podrá efectuarse a ficheros de titularidad privada sino con el consentimiento del interesado o cuando una ley prevea otra cosa.<sup>28</sup>

La Agencia de Protección de Datos española no se ha pronunciado aún claramente acerca de las relaciones entre ambos derechos. Es más, ha mantenido posturas contradictorias: la prevalencia de la normativa sobre acceso, la de la

---

28. Por lo demás, un cotejo de las disposiciones generales de creación de ficheros públicos permite comprobar que éstos no prevén la cesión de sus datos a sujetos privados, salvo que el fichero tenga precisamente por finalidad, exclusiva o concurrente, la información a los directamente implicados (como, p. ej., en materia de accidentes de tráfico).

normativa sobre protección de datos o la necesidad de un análisis caso por caso atendiendo al interés en juego y al principio de finalidad.<sup>29</sup>

Por su parte, la doctrina que ha analizado el derecho de acceso y se ha ocupado al hilo del estudio del régimen de los datos nominativos ha sido en general muy crítica con la exigencia de acreditación de un interés para acceder a los datos nominativos,<sup>30</sup> así como en los obrantes en expedientes sancionadores y disciplinarios,<sup>31</sup> obviando profundizar en el encaje de esta regulación con la

---

29. Así, en su Memoria de 1995 constata, en referencia a la cesión a particulares de datos del padrón, que la excepción de la exigencia de consentimiento por previsión legal, a que hacía referencia el artículo 11.2.a LORTAD, en conexión con el artículo 37.3 LRJAP-PAC, «determina que el acceso a datos personales podrá llevarse a cabo, además de por el titular, por terceros que acrediten un interés legítimo y directo, salvo las excepciones del apartado 37.4 de la misma ley». En esa misma Memoria, indica que las administraciones públicas consultan frecuentemente a la APD sobre las relaciones entre derecho a la protección de datos y derecho de acceso, señalando que «la respuesta debe valorarse caso por caso, poniendo en conexión la finalidad de los datos con el carácter de interesado del solicitante, junto con la pertinencia y el carácter adecuado de los datos para el ejercicio de los derechos del interesado». En la Memoria de 1996 afirma que el acceso por particulares a datos del padrón se rige por la LRJAP-PAC. En la Memoria de 2001, puede leerse: «Se informa también [de] que la posibilidad del derecho de acceso a los archivos y registros de las administraciones públicas, consagrado por el artículo 105.b de la Constitución y regulado por los artículos 35 y 37 de la Ley de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, tal y como reiteradamente ha señalado el Tribunal Supremo, no puede entenderse prevalente sobre la garantía del derecho fundamental a la protección de datos de carácter personal, quedando el acceso limitado en los supuestos en que los archivos y registros contuvieran datos de carácter personal a las previsiones reguladoras de la protección de datos. Así se desprende también de la doctrina sentada por nuestro Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre».

30. I. Villaverde Menéndez, *op. cit.*, p. 121, considera inconstitucional la restricción a los interesados del acceso a documentos meramente nominativos. Para S. Fernández Ramos, *op. cit.*, p. 105, la exigencia de acreditación de un interés para el acceso al resto de los datos nominativos no íntimos sería inconstitucional, en cuanto supone un límite sin acomodo constitucional, teniendo en cuenta que el nombre es un dato objetivo que no implica juicio de valor alguno que pueda atentar contra la intimidad de las personas. En definitiva, lo que parece una flexibilización en realidad sería una grave e injustificada restricción, al exigirse una especial legitimación. L. A. Pomed Sánchez, *op. cit.*, p. 466, estima que la limitación del acceso a los datos nominativos «puede vaciar de contenido el derecho de acceso, y es de una constitucionalidad más que discutible», ya que «entendido en su literalidad, el artículo 37.2 LAP convierte el ejercicio del derecho de acceso en una pura entelequia. En puridad, salvo algunos de los documentos contenidos en los expedientes confeccionados para la elaboración de disposiciones de carácter general, todos los documentos de la Administración tienen carácter nominativo». R. Parada Vázquez, *op. cit.*, pp. 165-166, se muestra crítico con la limitación en el acceso a los documentos nominativos, que parece en realidad servir a un deseo de evitar la transparencia de la actividad administrativa cara a los profesionales de los medios de comunicación.

31. Se ha dicho que este tipo de datos no pertenece a la intimidad de las personas y que, por ello, se trataría de una limitación inconstitucional, máxime cuando se contrapone al principio general

normativa sobre protección de datos. La que ha estudiado el tema desde la óptica de la protección de datos ha llegado, en ocasiones, a opiniones maximalistas conforme a las cuales no cabe en ningún caso la comunicación a terceros de ningún dato personal en poder de la Administración,<sup>32</sup> lo que nos parece que resulta absolutamente irreconciliable con el carácter no absoluto de los derechos fundamentales y su necesaria compatibilidad con el resto de derechos, bienes y principios constitucionales. Por ello es preciso, a nuestro juicio, un replanteamiento serio de la cuestión, que tenga en cuenta todos los derechos, principios y bienes en cuestión, y huya de planteamientos absolutos.<sup>33</sup>

Creemos que es posible formular una serie de *directrices*, a modo de decálogo, acerca de cómo habría de interpretarse la relación entre el derecho de acceso y el derecho a la protección de datos, la mayoría de las cuales se encuentran ya apuntadas o consolidadas en el derecho europeo y comparado,<sup>34</sup> pero no así en el español:

---

de publicidad del proceso penal (L. A. Pomed Sánchez, *op. cit.*, p. 467, que duda asimismo de la constitucionalidad de la exclusión de los expedientes sancionadores y disciplinarios), llegando a insinuarse (así Parada Vázquez, *op. cit.*, pp. 165-166) que esta restricción pretende, en realidad, evitar el control público sobre la potestad sancionadora y disciplinaria de la Administración. No obstante, hay posturas intermedias. Así, para C. Gay Fuentes (*Intimidad y tratamiento de datos en las Administraciones Públicas*, Complutense, Madrid, 1995) debería posibilitarse el acceso a la resolución administrativa que ponga fin al procedimiento, al menos previa omisión de los datos personales, como ocurre en los casos de las sentencias penales, mientras que, en opinión de S. Fernández Ramos, la limitación al acceso no puede en ningún caso extenderse a los que fueron parte en el procedimiento (ni, en su caso, al denunciante) y debe ceder en relación con aquellas sanciones respecto a las que se prevé expresamente su posible publicación. Finalmente, J. F. Mestre Delgado, *op. cit.*, defiende que en estos casos se conceda el acceso a los que acrediten la existencia de un interés legítimo, empalmando así, en realidad, con el régimen de los documentos nominativos en una interpretación *contra legem*.

32. Así, Lucas Murillo de la Cueva, P., *Informática y protección de datos personales (Estudio sobre la Ley orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993, p. 96, estima que la comunicación de datos desde ficheros públicos requiere, en todo caso, consentimiento del interesado, lo que equivale a negar el derecho de acceso a la información pública e incluso el derecho a la tutela judicial efectiva en el caso de documentos que incorporen información personal.

33. Sobre la dialéctica entre publicidad y reserva en el ámbito de los registros públicos y, en concreto, del Registro de la propiedad, nos remitimos a nuestra monografía *Publicidad registral y derecho a la privacidad. Una necesaria conciliación*, Centro de Estudios Registrales, Madrid, 2006, y al artículo «La publicidad registral a la luz de la normativa sobre protección de datos. En especial, las cuestiones jurídicas que plantea el acceso telemático al contenido de los libros del Registro», *Revista Crítica de Derecho Inmobiliario*, núm. 697, 2006.

34. *In extenso*, sobre el tema, con un estudio del derecho europeo, francés e italiano, nos remitimos a nuestro trabajo «La dialéctica entre acceso a la información en poder de la Administra-

1ª. Las relaciones entre publicidad y reserva de la información en poder de la Administración vinculada a personas determinadas ha de ser resuelta como todo conflicto entre valores, bienes, derechos y libertades constitucionales, mediante una delimitación del alcance y contenido de cada uno de ellos y una ponderación que permita compatibilizarlos en caso de conflicto, alcanzando la solución que en cada caso entrañe el menor sacrificio posible de cada uno de ellos.

2ª. Para la delimitación del alcance y contenido, debe tenerse en cuenta que la publicidad que se pretende al ejercitar el llamado «derecho de acceso» puede dar cobertura a finalidades diversas. El solicitante de acceso lo puede hacer como puro ejercicio de participación y control democrático (que es propiamente el fundamento del reconocimiento constitucional de este derecho) o bien como medio para la defensa de otros derechos o intereses. Por su parte, una información asociada al nombre de una persona puede afectar a ésta en su propia integridad física, en determinados supuestos (p. ej., información sobre funcionarios de prisiones), en su intimidad o en su derecho a la protección de datos, en casos en que se trata de información personal no íntima o en que pueden quedar afectados otros derechos dignos de protección que pueden conectar, en último extremo, con sus posibilidades de libre desarrollo de la personalidad y que instrumentalmente obtienen protección mediante el derecho a la protección de datos. Ahora bien, no toda información que contiene el nombre de una persona es un dato personal. El concepto de dato personal se ha extendido a toda información nominativa de cualquier género. Esta concepción omnicomprendensiva, justificada por la potencialidad lesiva del cruce de información nominativa que puede resultar «inofensiva» aisladamente considerada, comienza a ponerse en tela de juicio, y se apunta a los criterios del contenido, la finalidad y el resultado como guías para decidir cuándo una información asociada a una persona identificada o identificable es o no un dato personal.<sup>35</sup> Hay que partir, pues, de que no toda información que contiene el nombre de una persona es

---

ción y protección de datos personales», *Revista de Administración Pública*, núm. 173, mayo-agosto 2007.

35. Sobre el particular, son del máximo interés las cartas del Defensor del Pueblo europeo de 14 de noviembre de 2001, titulada «Transparencia y protección de datos («Openness and data protection»), y de 30 de septiembre de 2002, y, aún más, por la especialización y autoridad del órgano y su pretensión de reconducción de la interpretación del concepto de dato personal a escala europea, la Opinión 4/2007 del Grupo de trabajo sobre protección de datos del artículo 29 sobre el concepto de dato personal, adoptada el 20 de junio de 2007.

*ipso facto* información sobre dicha persona y, por ello, dato personal, y, por ende, que en muchos casos no se hallará en juego este derecho (ni, menos aún, el derecho a la intimidad). Dentro de los datos que sí dicen relación con una persona determinada, la normativa que regula el derecho de acceso presta una ayuda incuestionable para distinguir entre dato íntimo y dato nominativo. En especial ésta última, con su diferenciación de un régimen más garantista respecto a los datos denominados «especialmente protegidos» o «sensibles» (relativos a la ideología, creencia, religión, raza, vida sexual, salud, a los que se une un régimen también diferenciado de los datos sobre condenas penales o administrativas). Ciertamente, ni los datos íntimos —cuya definición no puede hacerse *a priori*, dada la congénita indefinición del concepto de intimidad—<sup>36</sup> se reducen a los especialmente protegidos, ni los datos especialmente protegidos tienen una conexión exclusiva con el ámbito de la intimidad (ya que se conectan a su vez con otros derechos, muy en especial, con el principio de no discriminación). Pero, en todo caso, la categoría de los datos especialmente protegidos supone una importante directriz para dilucidar cuándo una publicidad inconsentida por la vía del otorgamiento del acceso puede implicar una mayor injerencia en los derechos constitucionales de los afectados y, por ende, debe ser excepcional, sólo justificada por la prevalencia de otro derecho fundamental. Por el contrario, otro tipo de datos, como los «relacionales», fuera del ámbito familiar (laborales, económicos y, sobre todo, muchos de los referidos a relaciones con la propia Administración pública) caen fuera de esta protección reforzada pero pueden entrar en el concepto de dato personal. La ponderación, pues, entre publicidad y reserva ha de tener en cuenta, en consecuencia, cuál es el valor constitucional en juego en cada caso.

3<sup>a</sup>. La normativa reguladora del derecho de acceso a la información pública es la determinante de la legalidad o no de la comunicación de información que incluya datos personales desde la Administración a los ciudadanos, salvo cuando se trata del propio afectado, en cuyo caso es de aplicación la normativa sobre protección de datos, que regula el también denominado derecho de acceso y que bien pudiera calificarse, de forma probablemente más expresiva, como derecho de información individualizada (que, a su vez, ha de compatibilizarse en algunos casos con la protección del anonimato de terceros cu-

---

36. Sobre el particular, véase el análisis de la jurisprudencia constitucional y las reflexiones que le dediqué en el capítulo segundo de la monografía de Guichot, E., *Datos personales y Administración Pública*, *op. cit.*, y la bibliografía allí citada.

yos datos puedan figurar en dicha información). Esta regla debería tener consagración legislativa expresa, coordinando así bloques normativos en aras de la seguridad jurídica.

4ª. Tal y como apunta la normativa de acceso, los datos íntimos, en principio, deben ser los más resistentes a una publicidad inconsciente. No obstante, no puede excluirse tampoco de forma absoluta la publicidad de estos datos, cuando haya motivos de interés público o derechos individuales prevalentes, por lo que siempre es necesario un juicio *ad casum* (piénsese en la lucha contra los delitos, la protección de la integridad de las personas, la tutela de la salud, etc.). Por tanto, no cabe una exclusión *in genere y a priori* absoluta de la publicidad de este género de datos. Puede pensarse que, en estos casos, sobre una importancia decisiva cuál sea la finalidad de la pretensión de acceso: si está vinculada al control general de la actuación administrativa, basada en un principio de transparencia, o si está asociada a la necesidad de tutelar un bien o derecho constitucional diferente. Como apuntamos, en no pocas ocasiones la demanda de acceso no tiene por objeto el mero control de la actividad pública, sino que conecta con la efectividad de otro derecho fundamental del demandante (p. ej., información sobre ingresos de una persona a la Administración tributaria por su ex cónyuge o por sus hijos; demandas de datos sanitarios por personas que han sido contagiadas por el afectado; derecho a la igualdad en el acceso a la función pública, etc.). En estos casos, en realidad, el acceso es presupuesto para el ejercicio por el demandante de sus derechos constitucionales, y la ponderación ha de ser realizada, por tanto, entre el derecho en cuestión y el derecho a la protección de datos o, en su caso, a la intimidad (p. ej., dando en todo caso prevalencia al derecho a la vida y a la integridad física, en el supuesto de datos sanitarios). Es planteable si la normativa no debiera prever en estos supuestos que la revelación debiera someterse en todo caso, o salvo excepciones extremas en que esté en juego la integridad o seguridad de las personas, a autorización judicial, como ocurre con las manifestaciones «geográficas» de la intimidad (domicilio, comunicaciones).

5ª. En el caso de solicitudes de acceso a datos no íntimos, pero sí personales –categoría que debiera tender a la identificación con los «datos nominativos» de la actual normativa sobre acceso, hasta tanto no desaparezca esta categoría equívoca que ya ha sido suprimida en el derecho francés, del que se importó–, ha de valorarse, por una parte, la importancia que para la transparencia administrativa tiene en el caso concreto la concesión o denegación del acceso, sin olvidar lo dicho sobre que no todo dato que contiene el nombre de una per-

sona es un dato personal. Para este juicio habrá de tenerse en cuenta el tipo de información al que pretende accederse (p. ej., la información sobre actos emanados de la propia Administración, como licencias, ayudas o subvenciones concedidas, contribuye de forma clave e indiscutible a la transparencia administrativa, así como la relacionada con la identidad y actividades de agentes o contratistas de la Administración; no así, por ejemplo, el acceso al expediente disciplinario o a la declaración de la renta de un ciudadano cualquiera).<sup>37</sup> En la medida en que la información sea más reveladora del modo de administrar el bien común, mayor valor habrá de darse al interés por obtenerla. También conviene atender al sujeto que la reclama, en conexión con la finalidad de la demanda. Así, cuando son los profesionales de los medios los que tratan de obtener información respecto de la cual resulta clave el conocimiento de la identidad de una persona (p. ej., subvenciones recibidas por actividades empresariales desarrolladas por un alto cargo), en conexión con el papel estelar del derecho a la libertad de información como garantía del Estado democrático.<sup>38</sup> Como directriz puede apuntarse que cuando la información tenga directa conexión con la fiscalización pública de la actividad administrativa debe prevalecer, en principio, el derecho de acceso sobre el derecho a la reserva de los datos nominativos no íntimos. Por otra, habrá de medirse el perjuicio que pudiera causar al sujeto de los datos la revelación (para lo que habrán de ponderarse todas las circunstancias concurrentes, como el que hayan sido ya puestos de manifiesto previamente por el propio sujeto, los antecedentes –piénsese en revelar la dirección de correo electrónico de un funcionario que ha sufrido previas amenazas por este medio–, la actividad del sujeto –piénsese, p. ej., en desvelar la propia identidad de funcionarios de prisiones, asistentes sociales, etc., en determinados casos).

6ª. El juicio de proporcionalidad deberá llevarse a cabo conforme a las técnicas habituales en dicho género de razonamientos, elaboradas en especial

---

37. Resulta interesante constatar como, respecto de informaciones en materia de identidad, dirección, puesto de trabajo, etc., de funcionarios, o sobre subvenciones discrecionales, la legislación canadiense –a nuestro juicio, acertadamente– las excluye de la consideración como dato personal a los efectos de tratamiento y comunicación. Véanse, artículos 19 de la Access to information Act, R.S. 1985, c. A-1, s.1 y 3 y 8 de la Privacy Act, R.S.C. 1985, c. P-21.

38. En España, el Tribunal Constitucional ha afirmado que: «Las libertades del artículo 20 no son sólo derechos fundamentales de cada ciudadano, sino que significan el reconocimiento y garantía de una institución política fundamental, que es la opinión pública libre, indisolublemente ligada con el pluralismo político, que es un valor fundamental y un requisito del funcionamiento del Estado democrático» (STC 12/1982).

en el juicio constitucional.<sup>39</sup> Toda una serie de directrices procedimentales han de ponerse a su servicio. Las normas sectoriales pueden contribuir a dilucidar la cuestión, aclarando cuándo un dato personal recabado es susceptible *a priori* de ser objeto de posterior publicidad, informando al sujeto de ello, siempre que responda en efecto a una finalidad de transparencia que justifique, en abstracto, la restricción del derecho. En todo caso, debe tenerse en cuenta que el sujeto puede también en estos casos ejercitar el derecho de oponerse a dicha comunicación (que es una modalidad de tratamiento) que le garantiza la normativa sobre protección de datos cuando existan motivos fundados y legítimos relativos a una concreta situación personal. El juicio abstracto debe realizarse también a la hora de decidir, respecto a aquellos datos cuya publicidad se prevé, el medio y el soporte, a la luz de los potenciales riesgos para los derechos e intereses de los afectados. Aunque la no necesidad de motivar las solicitudes de acceso sea el principio general hoy vigente en nuestro derecho –si bien, otros derechos, como el italiano, sí lo exigen–, cabe plantearse si debe motivarse la solicitud de acceso, bien desde un inicio, bien a requerimiento de la Administración, si comprueba que la información solicitada incluye datos personales, para permitir una ponderación más afinada. Por la misma razón, habría de darse traslado de la solicitud de acceso al afectado (regulando los plazos), de manera que pudiera alegar lo que estimare oportuno acerca de la gravedad de la afectación a sus derechos que puede suponer la revelación de datos personales, o sobre la posibilidad de proceder a una previa anonimización.

---

39. Sobre el principio de proporcionalidad, en la doctrina española, véanse, entre otros, Barnés, J., *La propiedad constitucional. El estatuto jurídico del suelo agrario*, Civitas, Madrid, 1988, pp. 165-283; «El principio de proporcionalidad. Estudio preliminar», *Cuadernos de Derecho Público*, núm. 5, 1998, pp. 15-49; «Introducción al principio de proporcionalidad en el Derecho comparado y comunitario», *Revista de Administración Pública*, núm. 135, 1994, pp. 495-535; Cruz Villalón, P., *Derechos fundamentales y legislación*, pp. 233-245; «Nota: los derechos fundamentales», pp. 247-252, ambos recogidos en *La curiosidad del jurista persa, y otros estudios sobre la Constitución*, Centro de Estudios Políticos y Constitucionales, Madrid, 1999; Martín-Retortillo, L. y De Otto y Pardo, I., *Derechos fundamentales y Constitución*, Civitas, Madrid, 1988; Medina Guerrero, M., *La vinculación negativa del legislador a los derechos fundamentales*, Ed. McGrawHill, Madrid, 1996; «El principio de proporcionalidad y el legislador de los derechos fundamentales», *Cuadernos de Derecho Público*, núm. 5, 1998, pp. 119-141; Rodríguez de Santiago, J. M., *La ponderación de bienes e intereses en el Derecho administrativo*, Marcial Pons, Madrid, 2000; Villaverde, I., *Concepto, contenido, objeto y límites de los derechos fundamentales*, en *La democracia constitucional. Estudios en homenaje al profesor Rubio Llorente*, Congreso de los Diputados/Tribunal Constitucional/Universidad Complutense/Fundación Ortega y Gasset/Centro de Estudios Políticos y Constitucionales, Madrid, 2002, pp. 317-363.

7ª. Al estar en juego valores, bienes y derechos constitucionales, ha de intentarse su maximización. Por ello, habrá de procederse siempre al otorgamiento del acceso cuando mediante la anonimización de la información solicitada pueda alcanzarse dicha finalidad de conocimiento y control ya que, como establece la normativa sobre protección de datos, la información una vez despersonalizada cae fuera del ámbito de protección del derecho. No obstante, habrá de tenerse en cuenta que se considera dato personal, conforme a la citada normativa, toda información concerniente a personas físicas identificadas o identificables, de modo que la Administración habrá de cerciorarse de que la información despersonalizada que facilita no es susceptible de asociación. Asimismo, hay que considerar la posibilidad de conceder el acceso parcial, cuando determinadas partes de la información deban quedar reservadas a la vista del juicio de proporcionalidad emitido.

8ª. La decisión denegatoria habrá de ser, en todo caso, motivada, cuando restrinja derechos, sea el de acceso (y los derechos que se pretendan tutelar con la obtención de información, cuando el acceso es instrumental, como hemos expuesto), sea el derecho a la intimidad o a la protección de datos (o los derechos a los que instrumentalmente éstos contribuyen a tutelar). Así lo impone el artículo 54.1.a de la Ley 30/1992. Asimismo, debe ser notificada a los interesados, incluidos los sujetos afectados por la revelación de sus datos que supone la concesión del acceso a un tercero, como impone el artículo 58.1 de la citada Ley.

9ª. La institución de un organismo de control del funcionamiento del sistema de acceso a la información (bien burocrático en cada Administración, bien con la naturaleza de una Administración independiente), que pudiera pronunciarse sobre las decisiones administrativas, dando una respuesta rápida y gratuita (lo que resulta clave en materia informativa) y sentando gradualmente los criterios generales de ponderación, resulta clave en una materia como ésta en que la ley carece del mínimo grado de concreción. A falta de la misma, las agencias de protección de datos están llamadas a jugar un papel clave en el establecimiento de los criterios.<sup>40</sup> Evidentemente, como todos los actos administrativos,

---

40. Resulta seductora la idea de una reforma legislativa que extendiera la competencia de las agencias al acceso a la información –que incluiría un cambio de denominación. Esta solución podría ser tanto más conveniente en el caso de las agencias autonómicas cuya competencia se centra en los ficheros públicos y con una menor carga de trabajo que la AEPD. Es el modelo adoptado mayoritariamente por las provincias en Canadá.

las decisiones sobre acceso son susceptibles de control por los tribunales contencioso-administrativos, como establece el artículo 1.1 de la Ley 29/1998.

10ª. El tratamiento posterior de los datos personales queda sometido a la normativa sobre protección de datos.

Una valoración de la regulación contenida en el artículo 37 LRJAP-PAC, a la luz de estas directrices, nos sugiere las siguientes reflexiones:

– En lo que hace al régimen del acceso a los *datos íntimos*, se echa de menos una flexibilización de lo que aparece en la ley como un límite absoluto, ya que en ocasiones puede haber un interés público superior en la transparencia de actividades públicas relevantes, amén de que, como dijimos, en determinados casos la prohibición del acceso por terceros puede pugnar con la necesaria garantía de otros derechos fundamentales, muy en especial, con el derecho a la tutela judicial efectiva, pero no sólo (piénsese, p. ej., en la necesidad imperiosa que puede haber de conocer datos de salud de una persona para proceder al tratamiento médico de otra, en un supuesto de contagio), por lo que una exclusión radical, creemos, se enfrenta a la necesaria vigencia y ponderación de todos los derechos y bienes constitucionales en conflicto.

– Respecto a la exigencia de acreditación de un interés para acceder a *datos nominativos* –que, como dijimos, ha sido objeto de durísimas críticas por parte de la doctrina que se ha acercado al tema desde el estudio del derecho de acceso–, hay que señalar, no obstante, que a partir de las leyes de protección de datos y de la jurisprudencia constitucional en nuestro derecho todo dato referido a una persona identificada o identificable queda bajo el manto del derecho fundamental a la protección de datos, de modo que cualquier injerencia en el mismo (y la publicidad incontestada lo es) debe tener un fundamento constitucional y ser proporcionada. Lo dicho no implica, en modo alguno, que los documentos nominativos que no contengan información íntima (en la terminología legal) constituyan un límite infranqueable a las solicitudes de acceso. Pero se impone en el estado actual del derecho la necesidad de proceder a una ponderación, valorando si la demanda de acceso no encubre una mera investigación *ad personam* carente de legitimidad y no conectada con el principio de transparencia (esto es, una «finalidad incompatible» en los términos de la legislación sobre protección de datos). Esto es, cuando hay un dato personal, no hay consentimiento del interesado a su publicidad y el propio legislador no se ha pronunciado, no cabe otor-

gar el acceso automático a los mismos, sino acudir a un razonamiento en clave de proporcionalidad, siguiendo las pautas que antes hemos apuntado, en las que la naturaleza del dato y su desvinculación de lo íntimo son un criterio fundamental, pero no exclusivo. Al respecto, el principio de transparencia tendrá una especial consideración en los casos en que se trate de datos generados en el ámbito de la propia Administración, con sus agentes o con los ciudadanos, cuyo conocimiento sea necesario para el control de las actividades administrativas. La normativa sobre protección de datos no es tampoco ajena a la existencia de datos con «vocación de publicidad»: se trata fundamentalmente del nombre y apellidos, el domicilio, el número de teléfono y la profesión de las personas, en la medida en que aparezcan en las denominadas «fuentes accesibles al público».

– En cuanto al acceso a datos obrantes en *expedientes sancionadores o disciplinarios*, lo cierto es que la normativa europea y española sobre protección de datos otorga a los mismos una especial protección, consistente en que sólo pueden ser incorporados a ficheros públicos en los términos que establezcan las leyes, por lo que también a la luz de dicho bloque normativo parece justificarse una especial cautela en el acceso a datos que incorporan una valoración negativa y tienen, pues, un potencial lesivo para el sujeto. Ello no quiere decir que haya de denegarse el acceso en cualquier caso, pero sí que en estos supuestos debería ponderarse teniendo en cuenta esta consideración, de forma que sólo en casos en que su conocimiento sea esencial para el fin de transparencia y control, o bien exista en juego otro derecho o valor constitucional en la demanda de acceso, debería prevalecer la publicidad sobre la reserva.

Una reforma de la normativa sobre acceso debería, a nuestro juicio (y limitándonos al aspecto estudiado en este trabajo), tener en cuenta estos principios. Además, debería comenzar por incorporar una referencia clara al encaje entre dicha normativa y la reguladora del derecho a la protección de datos, en los términos expuestos, y en aras del principio de seguridad jurídica. Sería necesario regular el procedimiento, incorporando también las directrices antes mencionadas, por no hablar de la deseable creación de una autoridad en materia de acceso, cuya labor podría ser crucial, en general, y en todo caso a la hora de marcar pautas en la dialéctica publicidad-protección de datos.

A ello se suman los problemas de armonización de la regulación general del derecho de acceso establecida en el artículo 37 LRJAP-PAC con el régimen diseñado en la Ley 16/1985, de 25 de junio, de patrimonio histórico (comen-

zando, por cierto, por determinar a partir de qué momento del proceso archivístico es de aplicación una u otra).<sup>41</sup> Creemos que estos mismos principios han de ser de aplicación a los documentos obrantes en archivos históricos. El artículo 57 LPH dispone que si los documentos contienen datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la *intimidad de su vida privada y familiar* y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos. Como puede comprobarse, de una parte, una vez el documento forma parte de un archivo histórico, sólo se protege cuando afecte a su intimidad y en tanto no haya transcurrido un lapso temporal prolongado. Ahora bien, puede pensarse que tampoco en estos casos la prevalencia puede ser absoluta, sino que, cuando lo exija la efectividad de otro derecho o bien constitucional, habrá en su caso de proceder a la ponderación, en los términos y con las garantías antes indicadas. Lo que cabe plantearse es si la Ley de 1985 –anterior, por tanto, a la normativa sobre protección de datos– ha de entenderse como que cubre también los datos no íntimos pero sí personales (o «nominativos», en los términos de la LRJAP-PAC). A nuestro juicio, ha de responderse en armonía con los principios generales antes vistos. Parece evidente que la LPH, con su referencia a «la intimidad de la vida familiar y personal», permaneció sencillamente ignorante de lo que sería el posterior «nacimiento» del derecho a la protección de datos y que, por tanto, se precisa una interpretación armónica con las exigencias de él emanadas, en los términos expuestos. Además, es necesario coordinar la normativa sobre archivos con la normativa sobre protección de datos, en particular por lo que se refiere a la contraposición entre la finalidad de servicio a la documentación histórica de la investigación a la que sirve el sistema archivístico, de una parte, y la previsión de cancelación obligatoria de los datos una vez han cumplido con la finalidad para la que fueron recabados, junto a la previsión de que no son finalidades incompatibles a los efectos de la normativa sobre protección de datos los

---

41. De acuerdo con el art. 37.6.g LRJAP-PAC, se regularán por sus disposiciones específicas la consulta de fondos documentales existentes en los *archivos históricos*. Por su parte, el art. 57 LPH regula el acceso a los documentos concluida la tramitación de un documento, y tras el depósito y registro en los *archivos centrales* de cada entidad. Reconociendo que existe en este caso un defecto de técnica legislativa, creemos que la regulación más acorde con el sentido de la exclusión del art. 37.6.g LRJAP-PAC es la de reservar la aplicación del régimen de la LPH al acceso a documentos obrantes en archivos históricos.

tratamientos posteriores para fines históricos, estadísticos o científicos. En fin, esta necesidad particular se une a la más general de regulación de la normativa general del sistema archivístico, una gran falla de nuestro derecho.

En definitiva, se impone una auténtica reforma legislativa de la regulación de las relaciones entre publicidad y reserva en la normativa sobre acceso, reutilización, archivos y protección de datos que establezca la necesaria coordinación entre las mismas.

Ha de reconocerse, en efecto, que no es objeto propio de la jurisprudencia o de la Agencia definir *a priori* y en positivo acerca del respectivo contenido de uno y otro derecho. Desde luego, parte de su contenido terminará por delimitarse por vía «contenciosa». No faltarán tampoco construcciones doctrinales que contribuyan a esta tarea primordial. Al legislador, en todo caso, corresponde en primera instancia abrir camino en ese sentido, tanto mediante el establecimiento de una norma general sobre el derecho de acceso a la información administrativa –como se ha hecho en otros países, en la conciencia de que constituye el presupuesto elemental del ejercicio de tantos otros derechos y una premisa básica de la sociedad de la información–, cuanto indirectamente con la delimitación de otros derechos tendencialmente opuestos como el derecho a la protección de datos.

#### **IV. Conclusiones**

Hemos analizado en este trabajo las relaciones entre el derecho a la protección de datos y los principios de eficacia y transparencia administrativa, en relación con las comunicaciones de información que contengan datos personales y tengan por destinatarios sujetos públicos o privados. Se trata, a nuestro juicio, de un tema crucial del derecho público de la información necesitado de una profunda reflexión, que comienza a llevarse a cabo en el derecho europeo y comparado, pero que se encuentra casi virgen en nuestro derecho, en una orfandad legal, jurisprudencial y en gran medida doctrinal.

No nos hemos limitado a una labor de indagación en los materiales legales, jurisprudenciales –en sentido amplio– y doctrinales, sino que, además, hemos avanzado las directrices que, a nuestro juicio, deben disciplinar las relaciones entre eficacia, transparencia y privacidad. Y ello, puede decirse, a partir de un

axioma: la necesidad de compatibilización y ponderación de estos valores y, por tanto, de reconducción de una interpretación extrema del derecho a la protección de datos –propia, probablemente, de un primer momento de su construcción dogmática– que amenaza con lastrar de modo indeseable la posibilidad del flujo informativo necesario para la construcción de una Administración transparente y eficaz, por un mal entendido «fundamentalismo de la protección de datos», buena parte de cuya explicación está en la transposición mimética al ámbito del tratamiento administrativo de las técnicas de protección de la privacidad que tienen razón de ser en el ámbito de los tratamientos privados de información. En fin, una vez más se pone de manifiesto cómo la diferencia entre los sujetos, públicos y privados, por razón de los fines que persiguen –y que, en el caso de la Administración, justifican su existencia– marca el régimen jurídico a aplicar. Todo ello revela la absoluta pertinencia, la práctica necesidad, de la aprobación de una ley reguladora del tratamiento administrativo de la información. En todo caso, se trata de una materia por construir, y con estas páginas hemos tratado, modestamente, de aportar algunos materiales para el debate jurídico.

## RESUMEN

**Revista catalana de dret públic**, 35, ISSN 1885-5709, 2007

Fuente de la clasificación: Clasificación Decimal Universal (CDU)

Fuente de los descriptores: palabras clave facilitadas por los autores

342.721

Emilio Guichot Reina, profesor titular de derecho administrativo de la Universidad de Sevilla

### **es Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio**

p. 43-74

En este trabajo se analizan las relaciones entre el derecho a la protección de datos y los principios de eficacia y transparencia administrativa, en relación con las comunicaciones de información en poder de la Administración que contengan datos personales y tengan por destinatarios sujetos públicos o privados. Se trata de un tema crucial del derecho público de la información necesitado de una profunda reflexión, que comienza a llevarse a cabo en el derecho europeo y comparado, pero que se encuentra casi virgen en nuestro derecho, en una orfandad legal, jurisprudencial y en gran medida doctrinal.

El artículo no se limita a una labor de indagación en los materiales legales, jurisprudenciales –en sentido amplio– y doctrinales sino que, además, avanza las directrices que deben disciplinar las relaciones entre eficacia, transparencia y privacidad. Y ello a partir de un axioma: la necesidad de compatibilización y ponderación de estos valores y, por tanto, de reconducción de una interpretación extrema

del derecho a la protección de datos –propia, probablemente, de un primer momento de su construcción dogmática– que amenaza con lastrar de modo indeseable la posibilidad del flujo informativo necesario para la construcción de una Administración transparente y eficaz, por un mal entendido «fundamentalismo de la protección de datos», buena parte de cuya explicación está en la transposición mimética al ámbito del tratamiento administrativo de las técnicas de protección de la privacidad que tienen razón de ser en el ámbito de los tratamientos privados de información. En conclusión, una vez más se pone de manifiesto cómo la diferencia entre los sujetos, públicos y privados, por razón de los fines que persiguen –y que, en el caso de la Administración, justifican su existencia– marca el régimen jurídico a aplicar. Todo ello revela la absoluta pertinencia y la práctica necesidad de la aprobación de una ley reguladora del tratamiento administrativo de la información. En todo caso, se trata de una materia por construir a la que se ha tratado de aportar algunos materiales para el debate jurídico.

Palabras clave: derecho a la protección de datos; privacidad; intimidad; eficacia; transparencia; acceso a la información pública; tratamiento administrativo de la información.

**RESUM****Revista catalana de dret públic**, 35, ISSN 1885-5709, 2007

Font de la classificació: Classificació Decimal Universal (CDU)

Font dels descriptors: paraules clau facilitades pels autors

342.721

Emilio Guichot Reina, professor titular de dret administratiu de la Universitat de Sevilla

**es Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio**

ca Dret a la privacitat, transparència i eficàcia administrativa: un equilibri difícil i necessari

p. 43-74

En aquest treball s'analitzen les relacions entre el dret a la protecció de dades i els principis d'eficàcia i transparència administrativa, en relació amb la comunicacions d'informació en poder de l'Administració que continuen dades personals i que tinguin com a destinataris subjectes públics o privats. Es tracta d'un tema crucial del dret públic de la informació en què cal fer una profunda reflexió, la qual es comença a dur a terme en el dret europeu i comparat, però que es troba gairebé verge en el nostre dret, dins una orfandat legal, jurisprudencial i en gran manera doctrinal.

L'article no es limita a una tasca d'indagació en els materials legals, jurisprudencials –en sentit ampli– i doctrinals, sinó que, a més, avança les directrius que han de disciplinar les relacions entre eficàcia, transparència i privacitat. I això a partir d'un axioma: la necessitat de compatibilització i ponderació d'aquests valors, i, per tant, de reconducció d'una interpretació extrema del dret a la pro-

tecció de dades –pròpia, probablement, d'un primer moment de la seva construcció dogmàtica– que amenaça de llastrar de manera indesitjable la possibilitat del flux informatiu necessari per construir una Administració transparent i eficaç, per un mal entès «fonamentalisme de la protecció de dades», bona part de l'explicació del qual rau en la transposició mimètica a l'àmbit del tractament administratiu de les tècniques de protecció de la privacitat que tenen raó de ser en l'àmbit dels tractaments privats d'informació. En conclusió, una vegada més es posa de manifest que la diferència entre els subjectes, públics i privats, per raó dels fins que persegueixen –i que, en el cas de l'Administració, justifiquen la seva existència– marca el règim jurídic que cal aplicar. Tot això revela l'absoluta pertinència, la pràctica necessitat, de l'aprovació d'una llei reguladora del tractament administratiu de la informació. En tot cas, es tracta d'una matèria per construir a la qual s'ha tractat d'aportar alguns materials per al debat jurídic.

Paraules clau: dret a la protecció de dades; privacitat; intimitat; eficàcia; transparència; accés a la informació pública; tractament administratiu de la informació.

**ABSTRACT****Revista catalana de dret públic**, 35, ISSN 1885-5709, 2007

Classification source: Universal Decimal Classification (UDC)

Key words source: Key words are given by authors

342.721

Emilio Guichot Reina, tenured professor in Administrative Law at the University of Sevilla

**es Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio**en *The Right to Privacy, Transparency and Administrative Efficiency: a Difficult but Necessary Balance*

p. 43-74

This paper analyzes the relationships between the right to data protection and the principles of administrative efficiency and transparency, from the perspective of the communication of personal data in the possession of administrative agencies to public or private persons. This is a crucial issue in public information law, an issue that is need of deep rethinking. European and comparative law are beginning to reflect on this issue, but it is practically virgin territory in Spanish law. From a legal perspective, from the perspective of case law, and to a large extent, from the perspective of legal scholarship, this issue is an orphan.

The article does not restrict itself to an investigation of legal questions, broad issues of case law, and legal scholarship, but in addition, it puts forward the guidelines that should govern the relations between efficiency, transparency and privacy. And it does so based on one axiom: the need to reconcile these values, giving each of them their proportional weight, and, consequently, the need to redirect an ex-

treme interpretation of the right to data protection – an interpretation that probably prevailed at the outset, when it was dogmatically framed – that threatens to undesirably saddle the flow of information necessary for the construction of a transparent and efficient system of government administration with a misplaced “data protection fundamentalism.” To a large extent, this “data protection fundamentalism” can be explained by an imitative transposition of privacy protection techniques, which are justified in the domain of private information processing, to the area of government administration. In conclusion, the paper once again highlights how the difference between the ends pursued by public and private subjects, ends that actually justify the existence of government agencies, delimits the legal system to be applied. All of this reveals the absolute relevancy and the practical necessity of passing a law that would regulate the administrative processing of information. In any case, this is an area yet to be constructed; here we have tried to provide some material for the legal debate.

---

Key words: right to data protection; privacy; intimacy; efficiency; transparency; access to public information; administrative information processing.