LA PROTECCIÓN DE DATOS Y LOS AYUNTAMIENTOS

José Enrique Candela Talavero
Funcionario de la Administración local
con habilitación de carácter estatal
Secretario-Interventor del Ayuntamiento de Alcántara (Cáceres)

Extracto:

El artículo intenta presentar la consideración jurisprudencial del derecho a la protección de datos de carácter personal considerando su regulación en la LOPD 15/1999 y normativa de desarrollo, en relación con el derecho de acceso a los archivos y registros de las Administraciones públicas así como con las obligaciones impuestas a los ayuntamientos, especialmente con el tratamiento de los datos personales a través del padrón municipal.

Palabras clave: ayuntamiento, dato personal, acceso registros, padrón.

DATA PROTECTION AND MUNICIPAL COUNCILS

José Enrique Candela Talavero
Funcionario de la Administración local
con habilitación de carácter estatal
Secretario-Interventor del Ayuntamiento de Alcántara (Cáceres)

Abstract:

This article aims to focus on the case law of personal data protection considering its regulation in the LOPD 15/1999 and its development of rules, in relation to the right to access the files and registers of Public Administrations, and the responsibilities imposed to municipal councils, mainly in the treatment of personal data through the municipal census.

Keywords: municipal council, personal data, access to files, census.

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

Sumario

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

1. EL DERECHO A LA PROTECCIÓN DE DATOS: NORMATIVA Y NATURALEZA

La normativa sobre protección de datos está compuesta por la Ley Orgánica 15/1999, de 13 de diciembre (en adelante LOPD) [1], que transpuso a nuestro ordenamiento jurídico la Directiva 95/46/CE [2] y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

La aplicación de la LOPD exige una protección de la información personal que se maneja en toda actividad pública o privada, reconociendo unos principios de actuación, y contempla previsiones para un tratamiento correcto de los datos personales.

El órgano encargado de la vigilancia y control de la normativa sobre protección de datos es la Agencia Española de Protección de Datos (AEPD), regulada en el Título VI (arts. 35 a 42) de la LOPD, con competencia en todo el territorio nacional en materia de ficheros de titularidad privada y pública, y en aquellos territorios autonómicos en los que no se han creado agencias autonómicas de protección de datos, siendo los procedimientos tramitados ante la AEPD objeto de regulación en el Título IX del Reglamento 1720/2007 (arts. 115 a 158); agencia que considera este derecho en su *Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal* como: «El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos».

Pudiera parecer que determinada información recabada en la actividad pública, por ejemplo, la de índole fiscal, es más relevante a efectos de protección de datos personales, que la información personal sobre los vecinos. Sin embargo, esta última información tiene el carácter de derecho fundamental y está protegida por una ley orgánica, por tanto, tiene rango de protección más alto.

El artículo 1 de la LOPD dispone que su objeto es: «Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar».Con la protección de

[1] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14 de diciembre).

[2] Directiva 95/46/CE, de 24 de octubre, del Parlamento Europeo y del Consejo. Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE L 281, de 23 de noviembre).

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

datos se protege a las personas físicas y no a las personas jurídicas, pues se protege un derecho fundamental que hace referencia a la «privacidad» de las personas físicas.

A estos efectos, es dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables. Identificado el objeto, hay que considerar que el derecho a la protección de datos es un derecho fundamental que deriva del artículo 18.4 de la Constitución Española [3], y está reconocido por el Tribunal Constitucional (TC) como un derecho autónomo e independiente del derecho a la intimidad, más amplio que éste [también el Tribunal Superior de Justicia (TSJ) de Aragón en su Sentencia de 12 de mayo de 2008]. Así en la STC 292/2000, de 30 de noviembre [4], el TC definió el derecho a la protección de datos como «el derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal». En esta sentencia, este derecho fundamental: «... persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado», estableciendo, en cuanto a su ámbito, que «el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 de la Constitución Española otorga, sino los datos de carácter personal».

La STC 292/2000, de 30 de noviembre, realiza un esfuerzo diferenciador entre el derecho fundamental a la protección de datos personales y el derecho fundamental a la intimidad personal, pues siendo afines, se diferencian en la distinta función, ya que la finalidad del derecho a la protección de datos, teniendo un objeto más amplio que el derecho a la intimidad, se centra en habilitar a su titular una disponibilidad sobre el uso y destino de sus datos, e impedir así su divulgación lesiva a sus intereses. Además de por el objeto, se diferencian por el contenido, pues el derecho a la protección de datos concede al titular actuaciones positivas que imponen deberes de hacer a terceros que vulneren aquel derecho, en relación con la facultad de control mencionada, concretada en: el consentimiento previo, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.

Esta doctrina constitucional ha venido a materializarse en una norma internacional, como es la Carta de Derechos Fundamentales de la Unión Europea de Niza de 7 de diciembre de 2000, estableciendo su artículo 8 que «el derecho a la protección de datos de carácter personal es un derecho fundamental de los ciudadanos de la Unión». Desde esta perspectiva internacional, y la consideración de derecho fundamental que tiene la protección de datos personales, debe considerarse su proyección en acuerdos internacionales ratificados por el Estado español sobre la materia: el artículo 8.º del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (Roma), de 14 de noviembre de 1950, los artículos 5.º, 6.º, 8.º y 9.º del Convenio del Consejo de Europa para la

[3] El artículo 18.4 de la Constitución Española: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». La relación entre Derecho e informática, estudiada por PÉREZ-LUÑO, A.E., *Derechos humanos, Estado de Derecho y Constitución* y *Manual de Derecho Informático* (5.ª ed.) de DAVARA RODRÍGUEZ, M.A., Ed. Aranzadi, 2003.

[4] Sentencia 290/2000, 30 de noviembre, y Sentencia 292/2000, de 30 de noviembre (BOE 4 de enero de 2001). También SSTC 254/1993, de 20 de julio, y 202/1999, de 8 de noviembre.

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Estrasburgo), de 28 de enero de 1981, o en normativa europea como la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos, o el Reglamento (CE) número 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

En el ámbito subjetivo de la ley hay que considerar que un ayuntamiento (incluido en el art. 3.º de la LOPD), como responsable del fichero que decide sobre la finalidad, contenido y uso del tratamiento que se realiza de los datos personales, está obligado a garantizar la protección de los datos personales y para ello debe cumplir unas obligaciones. Por eso deberá elaborar una ordenanza municipal por la que se creen, modifiquen o supriman los ficheros de datos de los que es responsable.

Caso particular desde este ámbito subjetivo fue el pronunciamiento de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección 1.ª, Sentencia de 2 de julio de 2009, al incluir a los consejos reguladores, en su condición de Administración pública, por imponerlo así la orden por la que se aprueba el Reglamento de la Denominación de Origen Rioja al considerar que es un órgano desconcentrado del Ministerio de Agricultura, Pesca y Alimentación.

2. PRINCIPIOS Y OBLIGACIONES DE LA PROTECCIÓN DE DATOS

Las obligaciones que dan cumplimiento a los mandatos de la LOPD se pueden enumerar como sigue:

1. **Inscribir los ficheros en el Registro General de Protección de Datos**. Los ficheros de los que responde un ayuntamiento tienen titularidad pública y necesitan unos requisitos en su creación, modificación o supresión, bien en el Registro General de Protección de Datos de la AEPD, bien en el Registro de la Comunidad Autónoma correspondiente del territorio donde radique el ayuntamiento. Conforme al artículo 20 de la LOPD [5], la creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el

[5] Según el artículo 20 de la LOPD: «El contenido de la disposición de carácter general deberá hacer referencia a:

a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible».

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

«Boletín Oficial del Estado» o Diario oficial correspondiente. Artículo que también delimita el contenido de la disposición de carácter general.

En primer lugar, debe determinar los ficheros de los que es responsable, estudiando los tipos de datos de carácter personal que necesita en sus funciones, los usos de esa información o los terceros a los que va a ceder esos datos.

La LOPD [art. 3.º b)] define los ficheros de datos de carácter personal como «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso». Por su parte, el Reglamento 1720/2007, de 21 de diciembre, en su artículo 5.º 1 k), añade que «sea un conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados» [6].

Se pueden considerar como ficheros, por ejemplo, los ficheros de recaudación de cada uno de los tributos municipales, el fichero de padrón de habitantes, el de bolsa de empleo, o en su caso, servicios culturales cuando se ofrezcan estos servicios a través de la página web. A estos efectos no tienen la consideración de ficheros, y no están en el ámbito de la regulación y protección de datos de carácter personal, los libros bautismales. Así, la Sentencia del Tribunal Supremo (STS) de 19 de septiembre de 2008 recaída en el recurso de casación 6031/07, interpuesto por el Arzobispado de Valencia, anuló la Sentencia de la Audiencia Nacional de fecha 10 de octubre de 2007, que consideró los Libros de Bautismo como ficheros en los términos definidos en el artículo 3.º b) de la LOPD (en los mismos términos debemos mencionar la STS de 14 de octubre de 2008 y la Resolución de la AEPD núm. R/00261/2009, Procedimiento núm. TD/01064/2008, de 16 de febrero de 2009), para determinar que los Libros de Bautismo no tienen la consideración de fichero y no están sujetos a la legislación en materia de protección de datos.

La AEPD, en relación con la obligación de inscribir los ficheros en el Registro General de Protección de Datos, y contemplado en el artículo 39 de la LOPD, para materializar la previsión de un registro telemático, dictó dos resoluciones [7]. Se trata del Sistema de Notificaciones Telemáticas a la Agencia, a través del sistema obligatorio NOTA, que permite realizar las notificaciones de creación, modificación o supresión de los ficheros por vía telemática utilizando la firma electrónica [8].

2. **Garantizar la seguridad de los datos**. Es necesario tomar unas medidas de seguridad para proteger los datos personales de alteraciones, pérdidas, tratamientos o accesos no autorizados.

Para ello un ayuntamiento tiene que elaborar un documento que refleje las medidas que ha decidido adoptar para garantizar la seguridad de los datos de sus ficheros. Este documento, que debe-

[6] Para una definición detallada de los conceptos de la LOPD, Davara Rodríguez, M.A., «Guía práctica de protección de datos para Ayuntamientos», 1.ª edición, Octubre 2006, *El Consultor de los Ayuntamientos y los Juzgados*, págs. 45 a 58.

[7] Resoluciones ambas de 12 de julio de 2006, de la Agencia Española de Protección de Datos (BOE núm. 181, de 31 de julio).

[8] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

ría estar actualizado, es de obligado cumplimiento y tiene que ser conocido por los trabajadores municipales que usen información de carácter personal.

Sobre las medidas de seguridad, en cumplimiento del artículo 9 de la LOPD, y en relación con el tratamiento de datos en los ficheros no automatizados, hay que identificar e inscribir los datos en el Registro General de Protección de Datos de la AEPD o, en su caso, en el de la agencia autonómica que corresponda, cumpliendo todos los principios y obligaciones de la LOPD y, por otra parte, se deberán adoptar las medidas aplicables teniendo en cuenta las características de los ficheros. Así, en el caso de una carpeta archivada con un orden alfabético de apellidos estamos ante un caso de fichero manual o no automatizado que cumple con todos los requisitos para ser considerado como tal y por eso está en el ámbito de aplicación de la LOPD, medidas que buscan evitar así la alteración, pérdida o acceso no autorizado.

Esta seguridad queda violada al infringirse el deber de secreto (art. 10 de la LOPD) ante la actitud del ayuntamiento si procede a colocar en el tablón de anuncios copia de una denuncia en la que constan nombre, apellidos y documento nacional de identidad del denunciante, «divulgando de esta manera –dice la Sentencia de la Audiencia Nacional de 9 de mayo de 2008– datos de carácter personal sin ningún título que amparase tal revelación».

3. **Principios de actuación para un tratamiento legal de los datos**. Se hallan en los artículos 4.º a 12 de la LOPD, haciendo referencia, en primer lugar, a la **calidad de los datos**, que conforme al artículo 4 de la LOPD 15/1999 y artículo 8.º del Reglamento 1720/2007, de 21 de diciembre, implica que los datos sean adecuados, pertinentes y no excesivos en relación con el tratamiento que se va a realizar de ellos, así como ser exactos y actualizados. Así en el padrón de habitantes no hay que incluir datos que no sean necesarios para su finalidad como registro administrativo. A estos efectos la Audiencia Nacional en Sentencia de 7 de mayo de 2007 (FJ 2.º) declaró que «no puede un ayuntamiento utilizar datos personales para obtener valoraciones políticas de los gestores municipales o de la oposición, pues tal finalidad o uso no se corresponde con ninguna de las competencias municipales reconocidas en la ley», y terminó aclarando que «se ha realizado un uso incompatible de los datos personales del padrón municipal con aquella finalidad para la que fueron recabados, razón por la que se ha infringido el principio de calidad del dato en el sentido expresado anteriormente»; en segundo lugar, el **principio de información** (art. 5.º de la LOPD y arts. 18 y 19 del Reglamento 1720/2007), de manera que en la toma de datos se faciliten a su titular los datos de identidad y dirección del responsable del fichero y la información referente a la existencia de un fichero en el que van a ser incluidos los datos y la finalidad y destinatarios del mismo, así como sus derechos como titulares de los datos. De esta manera, en la página web de un ayuntamiento es necesaria la inclusión de la información mencionada en los formularios a través de los que se recogen datos, por ejemplo, para la inscripción en una actividad ofertada; en tercer lugar, tenemos el **principio de consentimiento** del titular de los datos, de manera que el responsable del fichero debe tener el previo consentimiento «inequívoco» de aquél para tratarlos. Consentimiento previsto por los artículos 6.º y 7.º de la LOPD 15/1999 y 12 a 17 del Reglamento 1720/2007, de 21 de diciembre, de manera que la solicitud del consentimiento deberá ir referida a un tratamiento específico, con delimitación de su finalidad y de las restantes condiciones que concurran para ese tratamiento, correspondiendo al responsable del tra-

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

tamiento la prueba de la existencia. Consentimiento que, en aras a la protección del titular del dato, se debe obtener de manera «inequívoca». Adjetivo previsto tanto por la ley nacional (art. 6.º 1 de la LOPD) como europea (art. 7.º de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995).

Ahora bien, este consentimiento, según Informes 60/2004 y 124/2008 de la AEPD, sólo se verá exceptuado en los supuestos contemplados en el artículo 11.2, entre los que cabe destacar aquellos casos en que una norma con rango de ley dé cobertura a la cesión, con la única excepción, tras la STC 292/2000, de 30 de noviembre, de que el cambio de finalidad esté fundado en una de las causas contenidas en el artículo 11 de la propia ley orgánica, pudiendo ser sustituida la necesidad del consentimiento para el cambio de finalidad por una previsión realizada en una disposición con rango de ley [art. 11.2 a)].

Como mecanismo de protección de la legalidad en materia de protección de datos, en el Título VII de la LOPD 15/1999 (arts. 43 a 49) se realiza una determinación de las infracciones y sanciones, calificando aquéllas en leves, graves y muy graves, al objeto de prever mecanismos de reacción ante la vulneración de las determinaciones de la propia ley, complementado con los artículos 120 y 121 de su Reglamento de desarrollo 1720/2007.

Así, la Audiencia Nacional, Sala de lo Contencioso-Administrativo, de 14 de abril de 2008, determinó cuándo existe infracción leve en relación con el deber de secreto del artículo 10 de la LOPD 15/1999 [9].

La AEPD en su Resolución de 2 de abril de 2008, en relación con la calidad de los datos, consideró que el Ayuntamiento de Huesca infringió el artículo 4.3 de la LOPD 15/1999, de 13 de diciembre, tipificando su actuación como grave, declarando que el «tratamiento» de datos personales exige que se lleve a cabo de conformidad con los principios de «calidad de los datos», es decir, que los datos tratados han de ser «exactos y puestos al día», requisitos que no se cumplieron. Asimismo, se puede considerar si estamos o no ante infracción grave, por la vulneración del deber de guardar secreto, en la Sentencia de 26 de noviembre de 2008, de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección 1.ª.

Y finalmente, considerar que fue impuesta como muy grave la sanción a la «Fundación Instituto San José y Unidad Editorial Internet, SL», por carecer de consentimiento en el uso de la imagen de una paciente, considerado como dato personal, en la Sentencia de 9 de julio de 2009 de la Audiencia Nacional. También muy grave fue la sanción impuesta a la empresa «Gas Natural Servicios SDG, SA», por la Sala Tercera del Tribunal Supremo, en Sentencia de 27 de enero de 2009, o por la Audiencia Nacional, de 30 de junio de 2004, por la cesión de datos personales de clientes de una empresa a otra del mismo grupo sin el consentimiento inequívoco de aquéllos.

[9] Artículo 10 de la LOPD. Deber de secreto: «El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.»

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

Otro supuesto de falta de consentimiento en la cesión de datos lo materializó la Sociedad General de Autores y Editores (SGAE) por grabar sin permiso una boda en Sevilla y aportar el vídeo a un juicio, lo que permitió a la AEPD multarla por ser aquélla una clara violación del derecho constitucional a la intimidad y a la propia imagen. Multa que, sin embargo, tras ser recurrida por la SGAE ante la Audiencia Nacional, quedó sin efecto al considerar ésta (Sentencia de 22 de abril de 2009) que «los datos no se incorporaron en un fichero de datos de carácter personal organizado y estructurado con arreglo a criterios que permitan el tratamiento de los datos, y por tanto hecho no incluido en el ámbito de aplicación de la normativa de protección de datos». Según la Audiencia Nacional, «la normativa de protección de datos ha de aplicarse solamente cuando hay un fichero de datos personales y la posibilidad de su tratamiento».

El consentimiento por regla general debe ser tácito, aunque será expreso cuando estemos ante datos sobre el origen racial, la salud o la vida sexual, y expresado por escrito cuando se trate de datos sobre ideología, afiliación sindical, religión o creencias; el principio del deber de secreto (art. 10 de la LOPD) supone la obligación del responsable del fichero y de todos aquellos que intervengan en cualquier fase del tratamiento de datos de guardar el secreto profesional respecto de los mismos. La información de carácter personal a la que se accede, en cumplimiento de sus funciones laborales, debe ser utilizada sólo dentro de sus competencias.

La aplicación cotidiana del principio de consentimiento a los efectos del uso de los datos de carácter personal se comprueba con la indebida práctica bancaria de cesión de datos al ayuntamiento correspondiente a los efectos recaudatorios correspondientes. La protección de datos tiene sus límites, y sobrepasarlos comporta incurrir en infracciones que se encarga de tipificar la LOPD como graves en el artículo 44.3 c), en relación a la vulneración del artículo 6.º 1 del mismo cuerpo legal [10].

Un supuesto de lo advertido fue la comunicación por Caja Navarra de datos como la entidad, oficina y cuenta corriente que el afectado mantenía abierta con dicha entidad financiera a un ayuntamiento, mediante la comunicación del código de su cuenta cliente (número de la entidad, número de la oficina, dígitos de control y número de cuenta de cargo) para que éste domiciliara en el futuro el recibo del Impuesto de Actividades Económicas (IAE), vulnerando así lo dispuesto en el artículo 4.º 2; pues que el afectado tuviera una cuenta abierta con la entidad financiera no facultaba a aquélla la cesión de sus datos al ayuntamiento, lo que provocó la sanción por la AEPD a la entidad Caja de Ahorros y Monte de Piedad de Navarra por una infracción del artículo 4.º 2 de la LOPD 15/1999, de 13 de diciembre, tipificada como grave en el artículo 44.3 d) de dicha norma [11].

En relación con este principio de consentimiento, el TS, en su Sentencia de 12 de abril de 2005, desestimó un recurso de casación interpuesto por un ayuntamiento y condenó a la citada corporación local por haber cedido datos personales sin consentimiento previo de los afectados, lo que supuso en

[10] Artículo 6.1 de la LOPD 15/1999. Consentimiento del afectado: «El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa». Artículo 44.3 c) de la LOPD 15/1999: Tipos de infracciones: «Son infracciones graves: proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible».

[11] Resolución de la AEPD de 13 de octubre de 2008. En el procedimiento sancionador PS/00209/2008, instruido por la AEPD a la entidad Caja de Ahorros y Monte de Piedad de Navarra.

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

este caso una infracción tipificada como muy grave en el artículo 43.4 b) de la LOPD (actuales arts. 6 y 46 de la LOPD). O la STS de 27 de enero de 2009 que declaró que «si bien es cierto que no puede exigirse para la obtención del consentimiento de los afectados, a la hora de tratar o ceder sus datos personales, que tal consentimiento se otorgue mediante correo certificado, al no estipularlo así ningún precepto de la normativa de aplicación, la persona física o jurídica que pretenda obtener tal consentimiento sí deberá arbitrar los medios necesarios para que no quepa ninguna duda de que efectivamente tal consentimiento ha sido prestado, es decir, que la cesión de los datos ha sido consentida de modo lo suficientemente claro para que no pueda interpretarse en otro sentido».

Por tanto, esta jurisprudencia delimita este principio de consentimiento, en relación con el carácter personal del dato integrado en un fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues el derecho a la intimidad es un derecho individual y no colectivo.

Con una finalidad de precaución y para evitar la vulneración del derecho a la protección de los datos de carácter personal por su uso negligente, en el trato diario con entidades financieras, se imponía una debida diligencia a estas entidades que reconoció la Audiencia Nacional [12] en su Sentencia de 18 de enero de 2002, estableciendo que «este deber comporta que el responsable (entidad bancaria, en este caso) de los datos tiene el deber de guardarlos, obligación que subsistirá aun después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo. Este deber supone que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto».

Existe otra figura además de la cesión o comunicación de datos, que es la de la prestación de un servicio contratado a un tercero que implique el acceso por ese tercero a los datos de un fichero del que es responsable el ayuntamiento, lo cual está previsto en el artículo 12 de la LOPD como un contrato de prestación de servicios en el que el tercero actúa como encargado del tratamiento respecto de los datos y debe sujetarse a las instrucciones que le indique el responsable del fichero para realizar única y exclusivamente los tratamientos que le sean encargados. Este contrato debe constar por escrito o en forma que permita acreditar su celebración y contenido, y tiene que cumplir con todas las exigencias de la LOPD.

4. **Atención al ejercicio de los derechos**. El titular de los datos de carácter personal tiene reconocidos unos derechos que le permiten limitar el tratamiento de sus datos, conocer su uso, actualizarlos y oponerse al tratamiento de los mismos sin su autorización.

Entre estos derechos, tenemos el de acceso, rectificación, cancelación y oposición, el derecho de impugnación de valoraciones, el derecho de consulta al Registro General de Protección de Datos y el derecho de indemnización por daños o lesiones en sus bienes o derechos sufridos por un tratamiento de datos no conforme a la LOPD. Su régimen jurídico se encuentra en el Título III de la LOPD que se desarrolla en los artículos 13 a 19 y en el Título III del Reglamento 1720/2007 (arts. 23 a 36); además, la AEPD dictó la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

[12] *Vid*. TSJ de Madrid (Sentencia de 19 de julio de 2001).

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

Junto al acceso a los datos de carácter personal, está el correlativo deber de secreto a que hace referencia el artículo 10 de la LOPD 15/1999, precepto que ha de ponerse en relación con el artículo 11.1 de la LOPD [13] que exige, con carácter general, el consentimiento del afectado para la cesión de sus datos, salvo en los supuestos contenidos en el apartado 2 del mismo artículo. Deber de secreto que motivó pronunciamientos jurisprudenciales como la Sentencia de la Audiencia Nacional de 14 de septiembre de 2001, al pronunciarse en estos términos: «este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española». En efecto, este precepto contiene un «instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos» (STC 292/2000). Este derecho fundamental a la protección de los datos persigue «garantizar al titular un poder de control sobre sus datos personales, sobre su uso y destino» (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, «es decir, el poder de resguardar su vida privada de una publicidad no querida».

Especial protección merecen los menores, en lo que a la protección de datos se refiere, lo que provocó la previsión de la LOPD que dictamina que no se pueden manejar datos de menores de 14 años sin el consentimiento de sus padres o tutores. Además, «los menores no emancipados no pueden pres-

[13] Artículo 11 de la LOPD 15/1999. Comunicación de datos.

«1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.
Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.»

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

tar el consentimiento para contratar y, por tanto, sin este requisito no es válido el contrato y no es susceptible de generar obligaciones».

Por esta razón intervino la AEPD sancionando a «Vodafone España, SA» por hacer un contrato telefónico con menores sin consentimiento de sus padres, por incluir sus nombres en el registro de morosos y por usar sus datos de manera irregular. Inscripción que sólo puede hacerse cuando hay una «deuda cierta, vencida y exigible» que haya resultado impagada. Esa deuda no era «cierta», ya que los contratos no eran válidos (Resolución de 18 de marzo de 2009).

El TS, en Sentencia de 11 de marzo de 2000, en relación con el IAE, declaró, en un caso de requerimiento de información a una compañía eléctrica sobre la potencia contratada por determinados clientes, que no existe vulneración del deber de confidencialidad sobre los datos objeto de tratamiento informatizado.

Mencionar que cuando estemos ante ficheros de los que sean responsables las Administraciones se estará,en cuanto al procedimiento y sanciones, a lo establecido en el artículo 46 de la LOPD. En este caso, el Director de la AEPD dictará una resolución, estableciendo las medidas que procede adoptar por la Administración infractora para que cesen o se corrijan los efectos de la infracción. También podrá proponer la iniciación de actuaciones disciplinarias, si procedieran.

Respecto al control de la actividad de los responsables de los ficheros que estamos tratando, podemos mencionar que se materializa con dos medios: autoridad de naturaleza administrativa –la Agencia de Protección de Datos– con funciones sancionadoras y preventivas (arts. 18, 44 y 45 de la LOPD), y empleando la vía jurisdiccional para buscar la anulación de la información obtenida ilícitamente, el cese de la actividad y, en su caso, la indemnización de daños y perjuicios ocasionados por la vulneración padecida por el titular de los datos personales (arts. 13 y 19 de la LOPD). Con el artículo 19.1 de la LOPD se da respuesta a la exigencia contenida en el artículo 23 de la Directiva 95/46/CE, a tenor del cual «los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido, sin perjuicio de que pueda ser eximido, total o parcialmente, de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño». Sobre este responsable, se pronunció la Audiencia Nacional para diferenciar al encargado de tratamiento y al sujeto externo o ajeno al responsable del fichero [14].

3. EL DERECHO AL ACCESO A LOS ARCHIVOS Y REGISTROS PÚBLICOS Y LA PROTECCIÓN DE DATOS (EL PADRÓN MUNICIPAL)

El artículo 105 b) de la Constitución Española establece que se regulará por ley el derecho al acceso a archivos y registros administrativos; así tenemos los artículos 35 h) y 37 de la Ley 30/1992,

[14] Con esta misma pretensión se dictaron por la Audiencia Nacional distintas sentencias (20 de septiembre de 2002 y 13 de abril y 18 de mayo de 2005).

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

de 26 de noviembre, reguladora del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante, LRJPAC); el artículo 18 e) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LRBRL); la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales (modificada por la Ley 48/1978, de 7 de octubre); la Ley 12/1989, de 9 de mayo, sobre Función Pública Estadística; la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT) (arts. 111 y 113), o la Ley 14/1986, de 25 de abril, General de Sanidad.

El artículo 35 h) de la LRJPAC reconoce entre los derechos de los ciudadanos, como antes hemos visto, el del acceso a los registros y archivos y, de forma más detallada, el artículo 37.1 de la LRJPAC establece que «los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión –gráfica, sonora o en imagen– o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud» [15].

La regulación del derecho de acceso a los archivos y registros supone un derecho a la transparencia administrativa, pero delimitado o protegido también por determinados secretos oficiales u otros derechos dignos de mayor protección y de ahí la larga y detallada regulación contenida en el artículo 37.

El principal obstáculo para el ejercicio ilimitado del derecho de acceso a archivos y registros puede venir de la colisión del mismo con otros derechos constitucionalmente reconocidos, singularmente el de intimidad (SSTSJ de Cataluña de 3 de mayo de 2000 y de Andalucía de 23 de diciembre de 1999).

Por ello, la ley tiene especial cautela en tal sentido, cuando afirma que «el acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del tiempo, conforme a los plazos máximos que determinen los diferentes procedimientos, de los que no pueda derivarse efecto sustantivo alguno». Por su parte, el apartado tercero del precepto parece querer ahondar en tal previsión al señalar que «el acceso a los documentos de carácter nominativo que sin incluir otros datos pertenecientes a la intimidad de las personas figuren en los procedimientos de aplicación del derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo».Por último, y como garantía definitiva, el apartado número cuatro señala que «el ejercicio de los derechos que establecen los apartados anteriores podrá ser denegado cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una ley, debiendo, en estos casos, el órgano competente dictar resolución motivada».

[15] Cfr. al respecto González-Varas Ibáñez, S.: *Tratado de Derecho Administrativo*, Tomo I, Aranzadi, 2008, págs. 90-96. González Navarro, F.: *Procedimiento Administrativo Local*, Tomo II, Iustel, 2005 págs. 358-365. Alonso Higuera, C.: *Manual del Secretario*, Tomo I, Atelier, 2002, págs. 164 y 165. Ballestero Fernández, A.: *Manual de Administración Local*, «Wolters-Kluwer España, SA», 2006, págs. 323 a 334. Parada, R.: *Derecho Administrativo II*, Ed. Marcial Pons, 2007, págs. 155 a 157.

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

Respecto de la forma de proceder al acceso a los archivos y registros, la ley vuelve a dar muestras de sus recelos, estableciendo condicionantes que, si son interpretados de forma amplia, pueden provocar una desnaturalización del derecho (en este sentido se pronunció la STS de 14 de noviembre de 2000). Así, se afirma en el artículo 37.7 de la LRJPAC que el derecho de acceso será ejercido por los particulares de forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos, para lo cual se establece como sistema general el de las peticiones individualizadas, quedando las solicitudes genéricas a la consideración con carácter potestativo de la Administración; si bien, esta regla admite una excepción en el caso de que los solicitantes sean investigadores que acrediten un interés histórico, científico o cultural relevante, supuesto en el que se podrá autorizar el acceso directo de aquéllos a la consulta de los expedientes, siempre que quede garantizada debidamente la intimidad de las personas. Así, reclamada indefensión en un trámite de aprobación de una ordenanza fiscal, fue denegada dicha alegación por el TSJ de Baleares (Sentencia de 24 de enero de 2003), pues solicitadas por el recurrente y no facilitadas por el ayuntamiento «copias de diversa documentación», se basa el Tribunal en que «a la incorporación a la tabla de derechos procedimentales de los ciudadanos de la obtención de copias de documentos contenidos en ellos –art. 35 a) de la LRJPAC– le son de aplicación los requisitos previstos en los apartados 7 y 8 del artículo 37 de la LRJPAC. Doctrina jurisprudencial que, tras ser recurrida, confirmó el TS en su Sentencia de 8 de mayo de 2009.

Por tanto, el derecho al acceso a archivos y registros encuentra limitaciones, ya que como declaró el TS en su Sentencia de 10 de junio de 1996: «Tal derecho de información genéricamente referido a cualquier actuación administrativa tiene especial relevancia en el campo del derecho urbanístico, donde el control de la observancia de la legalidad establecida, así como la de los planes y demás instrumentos de ordenación urbana, puede ser instada por cualquier ciudadano a través de lo dispuesto en el artículo 235 de la Ley del Suelo, de 9 de abril de 1976, aplicable al supuesto aquí enjuiciado. Pero, de acuerdo con el texto constitucional, el ámbito, contenido y límites de este derecho y la correlativa obligación de la Administración, respecto de la ordenación urbana, están expresados en el artículo 55.2 del citado Texto Refundido de la Ley del Suelo, al reconocer a todo administrado el derecho a que el ayuntamiento le informe por escrito, en el plazo de un mes, del régimen urbanístico aplicable a una finca o sector». Límites que también se encargó de establecer la STSJ de Castilla y León, de 15 de enero de 2007, aplicando el artículo 37.4 de la Ley 30/1992, la STSJ de Extremadura, de 21 de enero de 2003, declarando que «el ejercicio del derecho de acceso a los registros y archivos públicos, como ocurre con la mayoría de los derechos subjetivos, no es absoluto y encuentra una serie de limitaciones en atención a la protección de otros derechos e intereses públicos o de terceros».

Para delimitar este derecho y sus restricciones en relación con el padrón municipal hay que considerar los artículos 16 de la LRBRL y 53.1 del Reglamento de Población y Demarcación Territorial de las Entidades Locales, aprobado por el Real Decreto 1690/1986, de 11 de julio (RPDT), ya que el acceso a sus datos encuentra su limitación genérica en la posible violación de la intimidad personal así como de otros derechos fundamentales.

El registro administrativo *tiene el carácter de documento público y fehaciente para todos los efectos administrativos* (STS de 16 de diciembre de 1996), donde constan los vecinos de un munici-

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

pio, constituyendo sus datos prueba de la residencia y domicilio habitual en éste y ostentando las certificaciones que se expidan con relación al mismo carácter de documento público y fehaciente para todos los efectos administrativos. El artículo 17.1 de la LRBRL prevé: «La formación, mantenimiento, revisión y custodia del padrón corresponde al ayuntamiento, de acuerdo con lo que establezca la legislación del Estado».

El padrón crea una vinculación de la persona inscrita en el mismo, que afecta a su capacidad de obrar, afectando así al ejercicio de derechos y deberes respecto a ese ayuntamiento en concreto.

En el caso del padrón municipal, son muchos los conflictos que surgen respecto del acceso a su información, por los concejales, trabajadores o las empresas del municipio. El padrón municipal tiene una finalidad y unos usos de datos concretos y en ningún caso podrá ser libremente accedido por terceros o usada su información para finalidades distintas de las previstas en la norma que lo haya creado.

Desde la **perspectiva recaudatoria**, la confidencialidad quedará garantizada, porque se destina a un fin público con el objeto de asegurar la gestión recaudatoria, respecto de un concreto sujeto pasivo sin que vayan a revelarse aspectos que pudieran vulnerar los derechos fundamentales de la persona.

La individualización y concreción del sujeto pasivo nominativamente y a través de su número de identificación fiscal, así como su domicilio, son elementos necesarios para asegurar el ordenado ejercicio de aquella competencia de gestión y recaudación.

Se impone para la protección del interesado y la correcta aplicación de la LOPD una base de datos de contribuyentes, de la que se puedan obtener los padrones fiscales reales. No obstante, se deben señalar límites como:

- La vinculación de esa información a la sola ejecución de la competencia para la que se facilita y no otra.
- La captación de datos informáticos consistentes en nombre y apellidos, documento nacional de identidad/número de identificación fiscal y domicilio, se limitará a éstos, respetando la integridad del propio padrón de habitantes.
- Las comunicaciones de los interesados en relación a estos datos en cualquier fase del procedimiento recaudatorio (como, por ejemplo, fijación de un domicilio distinto a efectos de notificaciones) prevalecerán sobre la información proveniente del padrón municipal.
- Debe articularse el oportuno sistema de control por el funcionario responsable del servicio para garantizar el idóneo y específico uso al que se adscribe esa información, evitando la publicidad de la misma fuera de la unidad que la gestiona.

Hay dos ámbitos en los que la relación que se establece entre entidad local y ciudadano, en relación con la protección de datos, es más evidente:

REVISTA CEFLEGAL. CEF, núm. 108, págs. 69-88
Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

a) Elecciones locales. La Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG), prevé que cada término municipal constituye una circunscripción, atribuyéndole a cada municipio, según su artículo 179, un número de concejales dependiendo de la población que esté recogida en el padrón.

b) Hacienda local. Desde la perspectiva recaudatoria, el Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el Texto Refundido de la Ley Reguladora de las Haciendas Locales, señala que será en la participación del municipio en los tributos del Estado en función de su población (art. 111).

Se deben recordar los límites en el uso de los datos padronales, recogidos en la LRBRL 7/1985, en cuyo artículo 16.3 se dispone que: «Los datos del padrón municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública» [16].

Los datos del padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la LOPD 15/1999 y en la Ley 30/1992, de 26 de noviembre (art. 37). A lo que hay que añadir los preceptos constitucionales que funcionan como condicionantes máximos del uso de este derecho: artículo 16.2: «Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias»; artículo 18.1 y 4: «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen», «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»; o el artículo 24.2: «La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos».

En relación con la protección de los derechos constitucionales, y teniendo en cuenta el artículo 8.1 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, el TC (STC 110/1984, de 26 de noviembre) consideró que «no se considerarán intromisiones ilegítimas las actuaciones autorizadas o acordadas por la autoridad competente de acuerdo con la ley», añadiendo, «entiéndase que la ley sólo puede autorizar esas intromisiones por imperativos de interés público». En relación con el secreto estadístico, decir que disposiciones legales redundan en su protección; así, el artículo 36.4 de la Ley General de la Seguridad Social, aprobada por el Real Decreto Legislativo 1/1994, de 20 de junio, recoge que el deber de colaboración de los funcionarios públicos no alcanza al secreto de la correspondencia y al estadístico.

Por lo que se refiere a la **cesión de datos a un tercero distinto del interesado**, cabe indicar que tanto la LRJPAC, en su artículo 37.4, según el cual «el ejercicio de los derechos que establecen

[16] Resolución de 28 de abril de 2005 del Instituto Nacional de Estadística y de la Dirección General de Cooperación Local, por la que se dictan instrucciones técnicas a los ayuntamientos sobre el procedimiento para acordar la caducidad de las inscripciones padronales de los extranjeros no comunitarios sin autorización de residencia permanente que no sean renovadas cada dos años (BOE de 30 de mayo).

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

los apartados anteriores podrá ser denegado cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una ley, debiendo, en estos casos, el órgano competente dictar resolución motivada», como el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, en su artículo 9.4, disponen que «el ejercicio del derecho de acceso a archivos y registros y la obtención de copias de los documentos obrantes en poder de la Administración podrá ser denegado mediante resolución motivada cuando concurran razones de protección del interés público o de protección de intereses de terceros o cuando así lo disponga una ley».

En relación con esta previsión, debe ser objeto de mención por su trascendencia en el funcionamiento habitual de los ayuntamientos la previsión de respeto a la LOPD 15/1999 por la Administración en su actividad contractual, según reconoce la Ley de Contratos del Sector Público, Ley 30/2007, de 30 de octubre, en su disposición adicional 31.ª [17], de manera que no estaremos ante una cesión de datos, si se guardan las previsiones del artículo 12 de la LOPD 15/1999, cuando estemos ante datos que la Administración comunique al contratista para ejecutar el contrato, y supongan un uso de estos datos por éste en nombre de aquélla.

Se habilita la cesión de datos entre Administraciones en el artículo 21 de la LOPD 15/1999. De esta manera, si estamos ante datos obtenidos por la Administración local en el ámbito tributario de las personas jurídicas, dichos datos pueden ser comunicados de acuerdo a lo establecido en los artículos 93 a 95 de la LGT [18], salvo en los casos concretos que en ella se prevén, consagrando el carácter reservado de cuantos datos, informes o antecedentes obtenga la Administración tributaria en el desempeño de sus funciones. Si se obtiene en el ámbito de sus relaciones económicas (ficheros de acreedores)

[17] Disposición adicional 31.ª de la LCSP: «1. Los contratos regulados en la presente ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento.

En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha ley deberán constar por escrito.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que ésta hubiese designado.

El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.
b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.
c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento.»

[18] En este sentido se pronunció la AEPD en Informe 0316/2009 declarando «la existencia de un deber de colaboración con la Administración tributaria, que implicará la comunicación de los datos que revistan trascendencia tributaria y sean necesarios para el ejercicio por dicha Administración de las potestades que la ley le atribuye la aplicación del artículo 11.2 a) de la Ley Orgánica 15/1999, en conexión con el artículo 93 de la LGT».

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

éstos podrán ser cedidos a otras Administraciones de acuerdo con la legislación sectorial aplicable. Específicamente a estas cesiones hace referencia el artículo 94.5 de la LOPD al disponer que «la cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal». Si la cesión de datos fuera a la Administración de la Seguridad Social, se cederán en la recaudación de los recursos del sistema de la Seguridad Social, según los artículos 33 y siguientes del 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 en relación con el Real Decreto 1627/1995, de 6 de octubre, por el que se aprueba el Reglamento General de Recaudación de la Seguridad Social.

Respecto a la materia recaudatoria, en caso de facilitar información sobre los ficheros de los datos personales en orden a la gestión, liquidación y recaudación de los tributos, por el organismo que por delegación tenga encomendadas dichas competencias, esta gestión, liquidación y recaudación, de cuya responsabilidad no se hará responsable al ayuntamiento titular de los ficheros, sino a la Administración delegada y al personal afecto al servicio, por cuanto la cesión de los datos de los ficheros de la Diputación responde a lo previsto en la LOPD en su artículo 21.1, que al prohibir la cesión de datos de carácter personal elaborados por las Administraciones públicas para el desempeño de sus atribuciones, a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, está admitiendo la cesión cuando la misma lo es para el ejercicio de la atribución o competencia del titular del fichero, en este caso el ayuntamiento, por lo que el uso indebido que se haya hecho por la Diputación o las entidades y personal dependiente de la misma es responsabilidad ajena al ayuntamiento.

De otra parte, teniendo en cuenta que tanto el artículo 60 y siguientes del Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el Texto Refundido de la Ley Reguladora de las Haciendas Locales (TRLHL), relativos al Impuesto sobre Bienes Inmuebles (IBI), como los artículos 78 y siguientes de la misma ley, en relación con el IAE, en cuanto típicos supuestos de tributos que se gestionan a través de un padrón o matrícula, debemos, no obstante, diferenciar que no se menciona (como lo hacía el art. 91 de la LRHL 39/1988) en la normativa actual del Real Decreto Legislativo 2/2004 la puesta a disposición del público del padrón del IBI, por lo que debemos acudir a los artículos 50 a 54 del Real Decreto Legislativo 1/2004, de 5 de marzo, por el que se aprueba el Texto Refundido de la Ley del Catastro Inmobiliario, previéndose como regla general el acceso a los datos no protegidos en el Catastro, y reclamando, no obstante, para el acceso a datos protegidos (nombre, apellidos, razón social, código de identificación y domicilio de quienes figuren en el Catastro como titulares, o valor catastral) el consentimiento expreso, específico y por escrito del afectado, salvo en los supuestos contemplados en el artículo 53. Por contra, por lo que respecta al IAE, en el artículo 90.1 del Real Decreto Legislativo 2/2004 se establece que «la matrícula estará a disposición del público en los respectivos ayuntamientos».

En la cesión de datos entre Administraciones, la Audiencia Nacional, en su Sentencia de 1 de junio de 2005, consideró legal la cesión de datos entre los ayuntamientos y el registro de vehículos

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009

del Ministerio de Interior, atendiendo al carácter público del registro y habilitó el acceso por parte del ayuntamiento sin necesidad de consentimiento del afectado (y en parecidos términos la STS de 12 de noviembre de 1996). A estos efectos, mencionar la disposición adicional segunda número 2 de la LOPD 15/1999, en cuanto dispone que «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» [19].

Bibliografía

Alonso Higuera, C.: *Manual del Secretario*, Tomo I, Barcelona: Atelier, 2002, págs. 164 y 165.

Alonso Más, M.J.: «El Padrón Municipal», *Comentarios a la Ley Básica de Régimen Local,* coord. Domingo Zaballos, M.J., Ed. Thomson-Civitas, Cizur Menor (Navarra), 2005, pág. 326.

Ballestero Fernández, A.: «Manual de Administración Local», *El Consultor de los Ayuntamientos y los Juzgados*, Madrid, 2006, págs. 323 a 334.

Davara Rodríguez, M.A.: «Guía práctica de protección de datos para Ayuntamientos», 1.ª edición, *El Consultor de los Ayuntamientos y los Juzgados*, Madrid, octubre 2006, págs. 45 a 58.

García de Enterría, E. y Fernández, T.R.: *Curso de Derecho Administrativo,* II, 6.ª edición, Civitas, Madrid, 1993, pág. 467.

García Moreno, A.: «Impuesto sobre Bienes Inmuebles», *Comentario a la Ley de Haciendas Locales,* coord. Domingo Zaballos, M.J., Ed. Thomson-Civitas, Cizur Menor (Navarra), 2005, págs. 745 a 757.

González Navarro, F.: *Procedimiento Administrativo Local,* Tomo II, Madrid: Iustel, 2005, págs. 358-365.

González-Varas Ibáñez, S.: *Tratado de Derecho Administrativo,* Tomo I, Cizur Menor (Navarra).Thomson-Civitas, 2008, págs 90-96.

Jiménez Plaza, M.I.: «El Derecho de acceso a la información en el ámbito local», *Tratado de Derecho Municipal,* Tomo I, Dir. Muñoz Machado, S., Madrid: Civitas, 2003.

Parada Vázquez, R.: *Derecho Administrativo II*, Madrid: Marcial Pons, 2007, págs. 155 a 157.

Piñar Mañas, J.L.: «Protección de datos personales y Entidades Locales», *Reforma y retos de la Administración Local*, coord. Parada Vázquez, R. y Fuentetaja Pastor, A., Madrid: Marcial Pons, 2007, págs. 211 a 246.

Rivero Ysern, J.L.: *Manual de Derecho Local*, Cizur Menor (Navarra). Thomson-Civitas, 2004.

[19] *Vid*. Alonso Más, M.J., «El Padrón Municipal», *Comentarios a la Ley Básica de Régimen Local*, coord. Domingo Zaballos, M.J., Ed.Thomson-Civitas, Navarra, 2005, pág. 326.

Fecha de entrada: 16-10-2009 / Fecha de aceptación: 17-11-2009