

LA GACETA
DE LOS NEGOCIOS

DOCUMENTOS

de debe
para un me
miento de l
tuación, en la guía n
plazo de entrega del docu
ento en todo o en parte de
la jurisprudencia ordinaria a

DOSSIER

EL TRATAMIENTO DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS



LEGALIA ABOGADOS

El autor

LEGALIA ABOGADOS presta sus servicios a empresas e instituciones en todas las disciplinas del Derecho. Cuenta con equipos multidisciplinares, con un conocimiento de primera línea de los sectores a los que asesoran. El equipo del Departamento de Derecho de Tecnologías de la información se compone de distintas áreas de especialización entre las que destacan la contratación informática, protección de datos, comercio electrónico, propiedad intelectual, nombres de dominio y propiedad industrial, derecho audiovisual y de las telecomunicaciones.

LEGALIA ABOGADOS ha asesorado en materia de protección de datos en distintos niveles de la Administración Públicas de nuestro país, adquiriendo por ello una experiencia que le sitúa entre las firmas líderes en el sector. Este departamento está presente en todas las oficinas de la firma: Madrid, Barcelona, Oviedo y Valladolid. Gracias a la pertenencia a la red de despachos, Law Firm of the Americas y a la relación permanente con despachos europeos de prestigio en sus áreas de actuación, la firma extiende sus servicios a sus clientes en el extranjero.

Resumen

La adaptación del sector público a las nuevas tecnologías ha supuesto una mejora de la actividad administrativa en beneficio de la ciudadanía. Por ello, la relación entre la Administración Pública y el ciudadano es más cómoda y sencilla. Internet ofrece a los ciudadanos la posibilidad de tener un mayor conocimiento de novedades que se producen en el seno de la Administración e interactuar con la misma.

Sumario

- I. INTRODUCCION
- II.- NORMATIVA Y ÁMBITO DE APLICACIÓN
- III. FICHEROS DE TITULARIDAD PÚBLICA: CREACIÓN, MODIFICACIÓN, SUPRESIÓN, NOTIFICACIÓN E INSCRIPCIÓN.
- IV. DERECHOS DE LOS INTERESADOS EN RELACIÓN CON LOS DATOS PERSONALES EN PODER DE LAS ADMINISTRACIONES PÚBLICAS
- V. COMUNICACIÓN DE DATOS ENTRE ADMINISTRACIONES PÚBLICAS
- VI. EL CONTRATO DE ACCESO POR CUENTA DE TERCEROS A LOS DATOS CONTENIDOS EN FICHEROS DE TITULARIDAD PÚBLICA.
- VI. RESPONSABILIDAD DE ADMINISTRACIONES PÚBLICAS POR INCUMPLIMIENTO DE LA LOPD
- VII. SUPUESTOS CONCRETOS DE TRATAMIENTO DE DATOS PERSONALES APLICADOS A LA ADMINISTRACIÓN PÚBLICA.

I. INTRODUCCION

La introducción de las nuevas tecnologías e Internet en el sector administrativo ha tenido ventajas innegables. Sin embargo, en relación con el perfeccionamiento del funcionamiento y eficiencia del sistema, debemos ser conscientes que existen una serie de elementos que provocan incertidumbre y son fuentes de potenciales riesgos.

Las nuevas tecnologías pueden entrar en conflicto con el Derecho al Honor e Intimidad de las personas, derecho recogido en el Artículo 18 de la Constitución Española, que ha sido objeto de desarrollo mediante 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. Concretamente, debemos hacer referencia a su apartado cuarto que dispone que la Ley limitará el uso de la informática para garantizar el honor y el pleno ejercicio de sus derechos. Íntimamente relacionado con el mismo, se encuentra la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos que es uno de los instrumentos del que disponemos para defender nuestra intimidad y privacidad.

El riesgo en la seguridad de los datos puede concretarse cuando el propio administrado facilita o suministra una serie de datos de carácter personal a través de Internet o en el momento del tratamiento de las bases de datos informatizadas titularidad de la Administración.

II.- NORMATIVA Y ÁMBITO DE APLICACIÓN

La LOPD regula el tratamiento de aquellos datos de carácter personal registrados en soporte físico, que puedan ser susceptibles de tratamiento y su posterior uso o utilización tanto en el sector público como privado. La Ley excluye de forma expresa el ámbito referente a los ficheros mantenidos por personas físicas en el ejercicio de las actividades exclusivamente personales o domésticas, los ficheros sometidos a normativa sobre protección de materias clasificadas, ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Además de la iniciativa estatal, han sido varias las Comunidades Autónomas que, conscientes de la importancia que ha adquirido el correcto tratamiento de los datos personales, han creado sus propias Agencias y han desarrollado sus disposiciones legales. Tal es el caso de la Ley 8/2001, de 13 de Julio, de Protección de Datos de la Comunidad de Madrid, la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos o la Ley 5/2002, de 25 de febrero, de Ficheros de Datos de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos. No obstante, a diferencia de lo que sucede con la LOPD y su normativa de desarrollo, el ámbito de aplicación de dichas normas está limitado al tratamiento de ficheros de titularidad pública, de las respectivas Comunidades Autónomas.

III. FICHEROS DE TITULARIDAD PÚBLICA: CREACIÓN, MODIFICACIÓN, SUPRESIÓN, NOTIFICACIÓN E INSCRIPCIÓN.

Podemos definir los ficheros de titularidad pública como aquellos que recogen datos de carácter personal cuyo titular es una Administración Pública. Entre ellos se encuentran los de la Administración General del Estado; las entidades y organismos de la Seguridad Social; los organismos autónomos del Estado, cualquiera que sea su clasificación; las sociedades estatales y entes del sector público a que se refiere el artículo 6 de la Ley General Presupuestaria; las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros a que se refiere el artículo 40.2 de la Ley Orgánica 5/1992, de 29 de octubre; las entidades que integran la Administración local y los entes y organismos dependientes de la misma; y cualesquiera otras personas jurídico-públicas (Artículo 24, Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos).

La LOPD obliga a que los ficheros automatizados de datos de carácter personal, tanto en el ámbito privado como público, deban inscribirse en el Registro de Protección de Datos competente. Mientras que los ficheros de titularidad privada se registran en la Agencia Española de Protección de Datos, los ficheros de datos de titularidad pública deberán inscribirse en la Agencia Autonómica de Protección de Datos competente y, en caso de inexistencia, en la AEPD.

Siempre que exista un fichero que contenga datos de carácter personal, deberá seguirse el procedimiento legalmente establecido para su creación, modificación o cancelación, con la correspondiente notificación e inscripción en el Registro de la Agencia de Protección de Datos pertinente.

a) Creación, modificación y cancelación de ficheros públicos.

Tal y como establece el artículo 20.1 LOPD, la creación, modificación y cancelación de ficheros deberá realizarse mediante disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente.

Las disposiciones generales, que regulan la creación o modificación de ficheros públicos deben presentar el siguiente contenido:

- a) La finalidad del fichero y los usos previstos.
- b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarla.
- c) El procedimiento de recogida.
- d) La estructura básica del fichero y la descripción de los tipos de datos incluidos en el mismo.

e) Las cesiones y, en su caso, las transferencias internacionales.

f) El órgano administrativo responsable 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 exigible.

La cancelación de un fichero deberá realizarse igualmente mediante disposición general, dictada al efecto, regulando el destino de los datos, o en su caso, las previsiones que se adopten para su destrucción.

b) Notificación e inscripción de los ficheros de titularidad pública.

Todo fichero de datos de carácter personal de titularidad pública, deberá ser notificado a la Agencia de Protección de Datos competente, por el órgano de la Administración responsable del fichero, para su inscripción en el Registro de Protección de Datos. La notificación del fichero debe ser previa al tratamiento de los datos en ella contenidos.

Seguidamente, los ficheros de titularidad pública que hayan sido convenientemente notificados, serán inscritos de oficio por la Agencia de Protección de Datos, una vez ésta haya recibido copia de la disposición de creación, modificación o cancelación del fichero.

IV. DERECHOS DE LOS INTERESADOS EN RELACIÓN CON LOS DATOS PERSONALES EN PODER DE LAS ADMINISTRACIONES PÚBLICAS

La LOPD establece una serie de principios a los que debe ajustarse el tratamiento de datos de carácter personal, como la obtención del previo consentimiento del titular a dicho tratamiento, la necesidad de informar al mismo respecto del tratamiento que se va a realizar de sus datos, o la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición respecto de sus datos. En lo que respecta a estos principios y derechos, la necesidad de garantizar a sus titulares el cumplimiento de los mismos, es exigible, con independencia de la naturaleza pública o privada del responsable del tratamiento, si bien en este último supuesto concurren ciertas especialidades, especialidades que a continuación se enumeran:

a) El deber de información y deber de recabar el consentimiento por parte de las Administraciones Públicas

Las Administraciones Públicas están exentas de la obligación de requerir el consentimiento por parte del afectado, siempre y cuando los datos sean recabados en el ejercicio de sus competencias (Art. 6.2 LOPD). Esta exención no significa que el afectado

quede indefenso ante una actividad administrativa que vulnere su intimidad pues entra en juego el principio de calidad de los datos, vigente también para las Administraciones Públicas, que obliga a éstas a recabar y tratar únicamente aquellos datos que sean adecuados, pertinentes y no excesivos para el correcto ejercicio de sus competencias, no pudiendo destinarlos a finalidades distintas.

Esta excepción no exime a la Administración de la obligación de informar al afectado sobre los tratamientos de datos realizados. Así, el artículo 5 LOPD no diferencia entre que el responsable del tratamiento sea persona privada o pública, por lo que como regla general, deberá cumplir con lo establecido en dicho artículo. No obstante, de conformidad con lo dispuesto en el artículo 24.1 LOPD, las Administraciones Públicas quedarán exentas de la obligación de informar, cuando el cumplimiento de la misma afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales.

b) Los derechos de acceso, rectificación, cancelación y oposición.

Así mismo es obligación de las Administraciones Públicas articular los debidos procedimientos que garanticen a los titulares el ejercicio de los derechos de acceso, rectificación, cancelación y oposición que les reconoce la LOPD. No obstante, esta obligación está sujeta a ciertas excepciones recogidas en el artículo 23 LOPD, que afectan a los datos incluidos bien en ficheros policiales bien en ficheros de la Hacienda Pública, que serán objeto de análisis en epígrafes posteriores.

No obstante, como contrapartida a estas limitaciones, la LOPD atribuye al afectado la facultad de poner en conocimiento de la AEPD o la Agencia Autonómica en su caso, la denegación del ejercicio de estos derechos, para que su Director se pronuncie sobre la procedencia o no de la misma.

V. COMUNICACIÓN DE DATOS ENTRE ADMINISTRACIONES PÚBLICAS

En atención a lo dispuesto por el artículo 21 LOPD, debemos distinguir entre las comunicaciones de datos que se producen entre órganos de la Administración -tanto interadministrativas como intraadministrativas- y comunicaciones de datos recogidos de fuentes accesibles al público que tienen como destinatarios fichero de titularidad privada.

a) Comunicación de datos entre Administraciones Públicas

Como regla general toda comunicación de datos de una Administración a otra exige el previo consentimiento del interesado. Esta regla general admite una serie de excepciones al permitirse la comunicación de datos entre Administraciones Públicas sin recabar ese consentimiento en los siguientes supuestos:

- Cuando los datos sean comunicados para el ejercicio de competencias iguales o que versen sobre materias semejantes.

- Cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

- Cuando la comunicación tenga por objeto los datos que una Administración Pública elabore u obtenga con destino a otra.

A modo de advertencia hemos de hacer constar que la comunicación de datos entre órganos administrativos no exime del deber de informar, salvo en los casos en los que la Ley expresamente lo excepcione.

b) Comunicación de datos recogidos de fuentes accesibles al público de una administración pública a una persona privada

Para que se de este supuesto debe concurrir una doble condición:

1) Que la Administración que efectúa la comunicación de datos haya obtenido la información de fuentes accesibles al público, entendiendo como tales el censo promocional, los repertorios telefónicos en los términos previstos en su normativa específica, las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, los Diarios y Boletines oficiales y los medios de comunicación.

2) Que la comunicación de datos se efectúe con destino a ficheros de los que sea titular una persona o entidad privada.

Como regla general, cuando una Administración pretenda realizar una comunicación de datos en la que concurren estas circunstancias debe contar con el consentimiento de los titulares o, en su caso, estar autorizada por una Ley. Esto supone una excepción a la regla que rige para ficheros de naturaleza privada que no exige el consentimiento del titular de los datos contenidos en una fuente accesible al público para proceder a su cesión.

VI. EL CONTRATO DE ACCESO POR CUENTA DE TERCEROS A LOS DATOS CONTENIDOS EN FICHEROS DE TITULARIDAD PÚBLICA.

En ocasiones las Administraciones Públicas recurren a terceros para la prestación de servicios. Por este motivo, es posible que terceros accedan a datos de carácter personal que figuran en los ficheros de los que la Administración Pública es responsable. Dicho acceso puede darse, por ejemplo, en el supuesto de que un Ayuntamiento contrate los servicios de una empresa para que le gestione la tramitación de las multas, al no tener capacidad para ello. Este tratamiento es distinto a la figura de la comunicación de

datos que hemos analizado con anterioridad. Tal y como dispone el artículo 12 LOPD, no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

En la relación de encargado de tratamiento intervienen dos personas distintas:

- Responsable del Fichero: La persona, física o jurídica, responsable de decidir el tratamiento que se dará a los datos personales, que, en el caso que nos ocupa, será la Administración Pública. Asimismo, el responsable del fichero es el que facilita al encargado del tratamiento, los datos personales que éste último debe tratar (recoger, grabar, actualizar, conservar, modificar, bloquear o cancelar, entre otros) por cuenta del primero.

- Encargado del Tratamiento: La persona física o jurídica que lleva a cabo, sólo o conjuntamente con otros, el tratamiento (recogida, grabación, conservación, almacenamiento, modificación, actualización, cancelación o bloqueo, entre otros) de los datos personales por cuenta del responsable del fichero.

El acceso a datos por cuenta de terceros debe regularse a través de un Contrato que deberá presentar el siguiente contenido:

a) Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento;

b) Que no los aplicará o utilizará con fin distinto al que figure en dicho contrato;

c) Que los comunicará, ni siquiera para su conservación, a otras personas;

d) Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Así mismo, una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

VI. RESPONSABILIDAD DE ADMINISTRACIONES PÚBLICAS POR INCUMPLIMIENTO DE LA LOPD

El régimen de responsabilidad de las Administraciones Públicas por incumplimiento de la normativa en materia de Protección de Datos debe ser analizado en comparación con el que resulta de aplicación a los tratamientos de titularidad privada.

En efecto, dicha regulación viene a constituir una de las excepciones contempladas en la LOPD dando

lugar, a la exclusión de la potestad sancionadora e imposición de multas sobre el ente público infractor.

El artículo 46 LOPD estipula que cuando las infracciones a que se refiere el artículo 44 LOPD fuesen cometidas en ficheros de los que sean responsables Administraciones públicas, el Director de la AEPD dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

El artículo 43.2 LOPD apartado segundo matiza que, cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46.2 LOPD.

De forma expresa se prevé una excepción en lo que al procedimiento e imposición de sanciones se refiere cuando el incumplimiento afecte a ficheros de titularidad pública. En la práctica, se puede hablar de una inmunidad frente a las sanciones económicas.

Será el Director de la AEPD quien adopte las medidas oportunas que, en todo caso, darán lugar al dictado de una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. A pesar de preverse la notificación de dicha resolución al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera, resulta evidente que dicha medida es, en todo caso, más benévola que la que tendría lugar si la infracción se hubiera producido respecto de un fichero de titularidad privada.

Paralelamente, la Disposición Adicional Segunda del RD 1332/1994 establece que corresponde a las Comunidades Autónomas, respecto de sus propios ficheros, la regulación del ejercicio y tutela de los derechos del afectado y del procedimiento sancionador en los términos y con los límites establecidos en la Ley Orgánica 5/1992 (entiéndase hecha la referencia a la LOPD) y de acuerdo con las normas del procedimiento administrativo común.

La gestión de los incumplimientos de la normativa de Protección de Datos por parte de Administraciones públicas es asumida por las Agencias Autonómicas de Protección de Datos, y en su defecto, por la AEPD.

Asimismo, el Director de la AEPD podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

Junto con la resolución del Director de la AEPD, proponiendo las medidas de corrección previstas para que cesen o se corrijan los efectos de la infracción, también puede acordarse el inicio de actuaciones disciplinarias, en caso de proceder, actuaciones que irían dirigidas contra el funcionario o funcionarios cuya conducta haya dado lugar al incumplimiento de la normativa de Protección de Datos.

En particular, se prevé que las faltas cometidas por los funcionarios en el ejercicio de sus funciones, puedan ser tipificadas como muy graves, graves o

leves (artículos 6 a 8 del Real Decreto 33/1986, por el que se aprueba el régimen disciplinario de los funcionarios del Estado). La problemática surge a la hora de dar encaje a las conductas infractoras de los funcionarios con las infracciones definidas en el artículo 44 LOPD, lo que no siempre resultará sencillo y obligará a realizar una interpretación integradora.

Las sanciones disciplinarias (artículo 14 del RD33/1986) que pueden ser acordadas son:

- § La separación del servicio.
- § La suspensión de funciones.
- § El traslado con cambio de residencia.
- § El apercibimiento.

Se deberán comunicar a la AEPD las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores. El Director de la AEPD comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Dichas comunicaciones a la AEPD son preceptivas y en las mismas se deberá informar a ésta de las medidas que se hayan adoptado para, de manera efectiva, cesar y corregir los efectos de la infracción, así como informar de cualesquiera otros aspectos que, directa o indirectamente, guarden relación con el asunto.

VII. SUPUESTOS CONCRETOS DE TRATAMIENTO DE DATOS PERSONALES APLICADOS A LA ADMINISTRACIÓN PÚBLICA.

A continuación, una vez realizado un análisis general, estudiaremos unos supuestos específicos de especial relevancia en el ámbito del tratamiento de datos personales por parte de las Administraciones Públicas.

1. EL PADRÓN MUNICIPAL

La Ley 7/1985 de 2 de Abril, Reguladora de Bases de Régimen Local, define en el art. 16.1 el Padrón Municipal como el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo, y su gestión administrativa se llevará a cabo por los propios ayuntamientos con medios informáticos.

Por tanto, el Padrón Municipal es un fichero de titularidad pública, que deberá adecuarse al tratamiento que la LOPD establece específicamente para esta clase de ficheros. En primer lugar, se deberá declarar el fichero padrón a través de una disposición de carácter general, publicada en el BOE o Diario Oficial correspondiente, así mismo deberá procederse a su registro ante el Registro de la Agencia Autonómica correspondiente, o en su defecto en la AEPD.

No es necesario obtener el consentimiento de los ciudadanos para recabar y tratar sus datos por parte del Ayuntamiento, con el objeto de incorporarlos al Padrón Municipal, puesto que el ciudadano deberá inscribirse en el Padrón Municipal, por el mero hecho de vivir en España.

El Padrón Municipal, es uno de los ficheros de titularidad pública que presenta mayores problemas, y ello es por la gran cantidad de comunicaciones de los datos contenidos en el mismo. En este sentido, es necesario traer a colación la Recomendación 1/2004, de 14 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre la utilización y tratamiento de datos del padrón municipal por los Ayuntamientos de esta Comunidad Autónoma, que establece la normativa en materia de protección de datos sobre las comunicaciones de datos previstas en el Padrón Municipal.

A continuación se hará una síntesis sobre algunos supuestos específicos en materia de comunicación de datos del Padrón Municipal.

a) Cesión de datos a otras Administraciones Públicas.

La Administración peticionaria deberá acreditar y justificar dicha petición, estableciendo claramente la función que se propone realizar con los datos padronales. El Ayuntamiento podrá acceder a la petición, y ceder los datos adecuados, pertinentes y no excesivos para el cumplimiento de la competencia legítima de la Administración peticionaria.

b) Ficheros y Registros de Población de las Administraciones Públicas.

Se encuentra autorizada por Ley la cesión al Instituto Nacional de Estadística, a la Administración General del Estado, a la Autónoma y Local, cuya finalidad será constituir en las Administraciones solicitantes ficheros o registros de población para la comunicación de los órganos administrativos con los interesados residentes en sus territorios, siempre que ésta se realice dentro del ejercicio de sus competencias.

c) Cesión de datos con fines estadísticos:

Obligación de facilitar los datos patronales al Instituto Nacional de Estadística. Asimismo el INE deberá justificar previamente su petición en las funciones estadísticas reconocidas en la Ley: tipo de estadística a que va a destinarse, sus finalidades básicas y la norma que lo regula.

d) Cesiones de datos a instituciones y órganos jurisdiccionales.

No será necesario el consentimiento siempre y cuando la información tenga como destinatarios al Defensor del Pueblo, Ministerio Fiscal, Jueces o Tribunales, Tribunal de Cuentas, instituciones autonómicas con funciones análogas.

2. TRATAMIENTO DE DATOS POR LA ADMINISTRACIÓN TRIBUTARIA

La LOPD no ha querido permanecer ajena al tratamiento de datos de carácter personal por parte de la Administración Tributaria, tanto estatal como autonómica o local, que, en ejercicio de las competencias atribuidas por la Ley 58/2003, de 17 de diciembre, General Tributaria y demás normativa aplicable, es una de las que mayor volumen de información maneja.

Aunque la LOPD no dedica expresamente ningún artículo a los ficheros titularidad de la Hacienda Pública, de lo dispuesto en su artículo 23. 2, se desprende que éstos están sujetos a un régimen especial cuya peculiaridad consiste en la posibilidad de que sus Responsables denieguen el ejercicio de los derechos de acceso, rectificación y cancelación cuando éste obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso cuando el afectado esté siendo objeto de actuaciones inspectoras.

Para contrarrestar la potestad que este precepto atribuye a la Administración Tributaria, dejando a su libre arbitrio la apreciación de las circunstancias que justifican la denegación total o parcial de los derechos mencionados anteriormente, el artículo 23.3 LOPD faculta a los afectados para ponerlo en conocimiento del director de la AEPD o del Organismo competente de cada Comunidad Autónoma en caso de ficheros mantenidos por las Haciendas Autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

3. FICHEROS POLICIALES

La necesidad de salvaguardar el derecho a la protección de datos de carácter personal que asiste a los ciudadanos frente a posibles injerencias en su vida privada por parte de las Fuerzas y Cuerpos de Seguridad del Estado, en aras a la salvaguarda de la seguridad pública, ha hecho que, inicialmente, el legislador europeo y, con posterioridad, el nacional hayan querido regularizar esta situación.

En España, ha sido la LOPD la que ha asumido esta tarea, dedicando sus artículos 22, 23 y 24, que reproducen algunos de los principios recogidos en la Recomendación N R (87) 15 del Comité de Ministros del Consejo de Europa, de 17 de septiembre de 1987, relativa a la regulación del uso de datos personales en el sector policial, a los "Ficheros de las Fuerzas y Cuerpos de Seguridad del Estado".

Partiendo de lo dispuesto en el artículo 2 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, merecen la consideración de "Ficheros de las Fuerzas y Cuerpos de Seguridad del Estado" aquellos cuya titularidad corresponde tanto a las Fuerzas y Cuerpos de Seguridad dependientes del Gobierno de la nación (Policía Nacional y Guardia Civil) como a los Cuerpos de Policía dependientes de Comunidades Autónomas o Corporaciones Locales.

La LOPD, al referirse a estos ficheros, los divide en dos categorías (ficheros con fines administrativos y

ficheros con fines policiales), quedando sujetas a dos regímenes distintos.

Así, de un lado, los ficheros titularidad de las Fuerzas y Cuerpos de Seguridad del Estado que contienen datos de carácter personal recogidos con fines administrativos y de forma permanente están sujetos al régimen general de la LOPD de forma que los titulares de los datos en ellos incluidos disfrutan de plenas garantías respecto de los mismos.

En cambio, los ficheros creados por las Fuerzas y Cuerpos de Seguridad del Estado con fines policiales están sometidos a un régimen especial, que exceptiona la necesidad de informar a los titulares de los datos en ellos incluidos, contar con el consentimiento de los mismos y hacer efectivos sus derechos de acceso, rectificación y cancelación. Este régimen, censurado por la mayor parte de la doctrina, parece encontrar su justificación en la necesidad de que la aplicación del régimen general a este tipo de ficheros puede hacer peligrar las funciones propias inherentes a la actuación policial.

Las principales peculiaridades que presenta el régimen aplicable a los ficheros con fines policiales, giran en torno a las siguientes excepciones:

a) Excepción a la obligación de informar a los titulares de los datos

De lo dispuesto en el artículo 24.1 LOPD, declarado en parte inconstitucional por la STC 292/2000, de 30 de noviembre, se desprende que no será necesario informar a los interesados de los extremos previstos en los apartados 1 y 2 del artículo 5 LOPD, cuando esto afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales. Considera la doctrina mayoritaria que, la indeterminación de estos términos unida a la dificultad de probar su falta de concurrencia por parte de cualquier ciudadano que considere lesionado su derecho a la protección de datos, coloca a éste en una clara situación de indefensión frente a los órganos policiales.

b) Excepción a la obligación de solicitar el consentimiento de los titulares de los datos para proceder a su tratamiento

Dentro de esta excepción, el artículo 22 LOPD, engloba dos supuestos, uno aplicable a los datos personales en general (22.2) y otro a los datos especialmente protegidos (22.3). En el caso de que el tratamiento afecte a datos especialmente protegidos (origen racial, salud, vida sexual, ideología, religión, creencias o afiliación sindical), la LOPD parece exigir una mayor garantía, al condicionar dicho tratamiento exclusivamente a aquellos supuestos en los que sea absolutamente necesario para los fines de una investigación concreta.

c) Excepción a los derechos de acceso, rectificación, cancelación y oposición

El artículo 23.1 LOPD deja claro que las Fuerzas y Cuerpos de seguridad del Estado podrán denegar el

acceso, la rectificación o cancelación de los datos incluidos en sus ficheros en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Como contrapartida a este precepto, que concede a las Fuerzas y Cuerpos de Seguridad un amplio margen de discrecionalidad carente de controles efectivos, el artículo 22.4 LOPD, les obliga a cancelar los datos registrados con fines policiales cuando éstos dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento.

Próxima entrega: Landwell-PwC analiza la Ley de Mediación de Seguros.