GUTIÉRREZ CALVO, M., «Problemas jurídicos derivados de la aplicación del principio de calidad del dato por parte de las Administraciones Públicas», *REDUR* 11, diciembre 2013, págs. 169-198. ISSN 1695-078X

PROBLEMAS JURÍDICOS DERIVADOS DE LA APLICACIÓN DEL PRINCIPIO DE CALIDAD DEL DATO POR PARTE DE LAS ADMINISTRACIONES PÚBLICAS

Marcos GUTIÉRREZ CALVO

MÁSTER EN DERECHO DE LAS ADMINISTRACIONES PÚBLICAS
UNIVERSIDAD REY JUAN CARLOS

RESUMEN: En un mundo globalizado y altamente *informatizado* como el que nos ha tocado vivir, cobra especial importancia la denominada protección de datos de carácter personal, tanto por las Administraciones Públicas como por los particulares –ya sean personas físicas o jurídicas–, toda vez que nunca hasta este momento los datos íntimos han estado expuestos a una publicidad como la que presenta la red de redes. En este sentido, uno de los principios que integran el Derecho de la Protección de Datos es el principio de calidad del dato, el cual intentaré definir así como realizar un análisis de la problemática de la aplicación del mismo por parte de las Administraciones Públicas.

PALABRAS CLAVE: protección de datos, principio de calidad del dato, Administraciones Públicas.

ABSTRACT: In a globalized and highly computerized world like the one we live, the so–called protection of personal data is of special importance, both by government and by individuals –whether individuals or corporations–, since never before intimate data have been exposed to the publicity that the network of networks represents. In this sense, one of the principles that comprise the Data Protection Act is the principle of data quality, which I try to define as well as to perform an analysis of the problems of its application by the public administrations.

KEYWORDS: data protection, principle of data quality, public administrations.

I. Breve introducción

El objeto del presente trabajo jurídico no es otro que el de poner de manifiesto la problemática en la aplicación del principio de calidad del dato en el devenir diario de las actuaciones de las diferentes Administraciones Públicas –Administración General del Estado, Comunidades Autónomas, Entidades Locales, Administración institucional y Administración corporativa– a través de ejemplos concretos.

Para lograr tal objetivo, he venido realizando una labor investigadora acudiendo a diversas fuentes de variada tipología, como manuales de Derecho Administrativo, monografías jurídicas, artículos de revistas especializadas, bases de datos de resoluciones administrativas, jurisprudencia, legislación, dictámenes de organismos públicos, etc.

En primer lugar, intentaré definir –si es que esto es posible– el concepto de calidad de los datos, para seguidamente profundizar en cada uno de sus aspectos o notas caracterizadoras desde un punto de vista amplio.

En segundo lugar, analizaré diferentes supuestos de aplicación de dicho principio a situaciones administrativas concretas desde el punto de vista de las Administraciones Públicas y la problemática que presenta. En este sentido, realizaré un análisis de una selección de diferentes informes jurídicos y resoluciones tanto de la Agencia Española de Protección de Datos como de la Agencia de Protección de Datos de la Comunidad de Madrid –actualmente extinta–.

En tercer lugar, aporto una breve reflexión personal sobre la aplicación administrativa de dicho principio jurídico, basándome en el común de supuestos analizados con el fin de extraer conclusiones.

Finalmente, incluyo un recopilatorio de la bibliografía y otros materiales empleados en la elaboración del presente trabajo de investigación.

II. Aproximación al concepto de calidad del dato

En una primera aproximación, intentaremos dar una definición al concepto de calidad de los datos enmarcado dentro de los principios de la protección de datos del Título II de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298 de 14.12.1999; en adelante: LOPD).

En concreto, dicho principio se encuentra regulado en el artículo 4 de dicho texto legal con el alcance siguiente:

Los datos de carácter personal sólo pueden utilizarse o tratarse cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que han sido obtenidos.

Asimismo, aquellos datos que se hubieran obtenido para su tratamiento, deben ser exactos y siempre estar actualizados, de manera que respondan en cualquier momento a la situación concreta y actual de la persona física titular de los mismos.

Dichos datos, deben ser obtenidos y tratados de forma leal y lícita, por esta razón se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Cuando los datos de carácter personal sean recogidos directamente del propio interesado, se consideraran

exactos los proporcionados por éste.

Tampoco podrán usarse para finalidades incompatibles con aquellas para las que los datos de carácter personal hubieran sido recogidos.

Los datos de carácter personal deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados y sólo podrán conservarse durante el tiempo en que pueda exigirse alguna responsabilidad derivada de una relación u obligación jurídica o derivada de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Por su parte el Reglamento de desarrollo de la Ley, el Real Decreto 1720/2007 de 21 de diciembre (BOE núm. 17, de 19.01.2008; en adelante: RPD), en su artículo ocho viene a confirmar lo ya apuntado con respecto a la Ley, pero regulando con un mayor grado de detalle los procedimientos en esta materia.

En este sentido, establece un plazo de diez días para la cancelación y sustitución de oficio de los datos inexactos o incompletos, en todo o en parte, por los nuevos datos rectificados o completados, salvo que la legislación sectorial establezca procedimiento o plazo distinto; debiendo asimismo notificar en su caso al cesionario las actuaciones efectuadas en igual plazo, siempre que fuere conocido, debiendo este actuar en el mismo sentido en el plazo de diez días desde la recepción de la notificación, no procediendo la comunicación y sin perjuicio del ejercicio de otros derechos por parte del interesado.

En el caso de los ficheros policiales, tal y como plantea TRONCOSO REIGADA[1], existe una matización en el artículo 22.2 de la LOPD, en el sentido de que se permite la existencia de ficheros con diversos grados de fiabilidad debido a la especialidad de la función investigadora policial, flexibilizando el cumplimiento de las exigencias de la LOPD en cuanto al consentimiento de los interesados en los supuestos de categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

Sobre la conservación de los datos cuando hayan dejado de ser necesarios o pertinentes, el Reglamento dice que una vez agotado el plazo en el que pueda exigirse algún tipo de responsabilidad jurídica o contractual, sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la LOPD y en el mismo Reglamento.

Finalmente, los ficheros deberán permitir en todo caso ejercer el derecho de acceso en tanto no proceda su cancelación.

II.1. Adecuación, pertinencia y no excesividad de los datos personales

Esta primera nota del principio de calidad de los datos viene a significar que la LOPD prohíbe el tratamiento de datos que no sean necesarios para atender a la finalidad que se autoriza, aunque el interesado haya prestado su consentimiento informado, introduciendo por lo tanto un nuevo límite *ex lege*, que se ve reflejado en diversas

[1] TRONCOSO REIGADA, A., «Principios de la Protección de Datos: el principio de calidad de los datos (Iª parte)», en TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Iª edición, Madrid, Civitas, 2010, pág. 16, *in fine*.

disposiciones como el artículo 15 del RPD que establece previsiones relativas al uso de los datos para finalidades no relacionadas directamente con la ejecución del contrato, así como en el artículo 65 del Real Decreto 424/2005 de 15 de abril, que aprueba el Reglamento sobre las Condiciones para la Prestación de Servicios de Comunicaciones Electrónicas, el Servicio Universal y la Protección de los Usuarios (BOE núm. 102, de 29.04.2005; en adelante: RSUT).

En este sentido, el tratamiento de los datos de facturación telefónica presenta un gran interés para las compañías de dicho sector, no solamente por la obvia finalidad retributiva sino por un interés estadístico orientado hacia la prospección y su posterior explotación comercial del perfil económico del cliente, sus necesidades y tendencias de consumo, tal y como menciona APARICIO SALOM.[2]

Por su parte, el artículo 15 del RPD obliga al responsable del tratamiento a facilitar el ejercicio del derecho de oposición expresa del interesado para destinar dichos datos a otra finalidad distinta que la de ejecución del contrato, permitiendo que dicha formalidad se lleve a cabo mediante una casilla que no se encuentre previamente marcada en el contrato.

A mayor abundamiento, el artículo 16 del RPD se refiere específicamente al tratamiento de datos de tráfico y facturación, remitiendo al artículo 65 del RSUT, que establece la obligación de eliminar o despersonalizar los datos de tráfico una vez terminado el servicio de telecomunicaciones, o cuando transcurra el plazo en que pueda impugnarse la factura o exigirse el pago.

Dicho esto, el apartado 3 de dicho precepto facilita a las operadoras la explotación de dichos datos para fines de prospección comercial y de oferta de servicios de valor añadido durante el tiempo necesario, una vez recabado el consentimiento informado del cliente, para el que opera la presunción de silencio positivo –al igual que en el RPD–, debiendo informarle previamente de los tipos de datos de tráfico objeto del tratamiento, así como de su duración.

Hay que destacar que no todo consentimiento del interesado convalida cualquier tratamiento que vaya más allá de la finalidad para la que fueron recabados los datos (datos excesivos o publicación *abierta* en Internet), por ejemplo, en el caso de que se supedite la concesión de un beneficio (subvención, beca, ayuda, etc.) al consentimiento informado, éste podría estar viciado por no ser un consentimiento libre, tal y como exige el artículo 3 h) de la LOPD.

En tal sentido, no es exagerado decir que dentro del principio de calidad de los datos, se encuentran los principios de adecuación, de exactitud e integridad de los datos y de prohibición de exceso en su recogida.

II.1.1. El principio de adecuación

Sobre el principio de adecuación, hay que aclarar que en lo que interesa, es lo

[2] APARICIO SALOM, J., «La calidad de los datos: Título II. Principios de la Protección de Datos, artículo 4», en TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Iª edición, Madrid, Civitas, 2010, pág. 4.

mismo que decir principio de idoneidad o principio de pertinencia, de tal manera que para que un fichero cumpla con el principio de calidad de los datos, es necesario que exista una idoneidad entre los datos recabados y la finalidad del mismo, debiendo cumplirse ésta con el tratamiento de los datos recabados.

A mayor abundamiento, la finalidad del fichero debe ser legítima, por lo que para valorar el cumplimiento de este principio se hace necesario analizar la misma, que será la que determine qué datos son susceptibles de ser recogidos y cuáles no cumplen este requisito.

II.1.2. El principio de exactitud e integridad de los datos.

En cuanto al principio de exactitud e integridad de los datos, es especialmente importante la actualización continua de los datos contenidos en el fichero con la finalidad de respetar el principio de calidad, de tal manera que sean exactos y se encuentren puestos al día, reflejando la realidad del sujeto, lo que obliga al responsable a disponer de procedimientos que garanticen dicha actualización.

Pensemos en la importancia de esta actualización en el caso del padrón municipal, ya que puede afectar incluso a derechos fundamentales, como el derecho de sufragio activo, y a otros derechos, como la percepción de ayudas sociales o económicas, o el derecho a la sanidad y a la educación, entre otros, amén de afectar a la propia función administrativa, así como a la propia organización municipal –número de concejales u obligación de prestar servicios públicos conforme a la Ley 7/1985 de 2 de abril, reguladora de las Bases de Régimen Local (BOE núm. 80, de 03.04.1985; en adelante: LBRL).

Las infracciones en estos casos son tipificadas como graves por el artículo 44.3 f) de la LOPD. Por otro lado, se consideran exactos los datos que reflejen hechos constatados con ocasión de la tramitación de un procedimiento administrativo, así como los facilitados por el interesado para dicha tramitación, según el artículo 8.5 del RPD.

En el ámbito de la administración electrónica, la Ley 11/2007 de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos (BOE núm. 150, de 23.06.2007; en adelante: LAECSP), en su artículo 4 h), establece un principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos, de gran importancia en los registros y notificaciones telemáticas por obvias razones.

Mayor importancia cobra, si cabe, la garantía del principio de exactitud en los denominados ficheros públicos o de acceso generalizado, donde la falta de actualización hace que pierdan tal carácter[3] lo cual impide su tratamiento sin consentimiento del interesado. A modo de ejemplo, es el caso de los listados de colegiados en los Colegios Profesionales en los que se exige al responsable del fichero que informe gratuitamente que dichos datos no pueden ser utilizados para fines publicitarios o de prospección comercial.[4]

En cuanto a los ficheros privados de solvencia patrimonial y crédito, la LOPD permite que los prestadores de dichos servicios puedan tratar los datos obrantes en los ficheros de acceso público sin consentimiento previo de los afectados, lo que supone no

[3] Véase artículos 6.2 y 11.2 b) de la LOPD.

[4] Véase artículo 28.2 de la LOPD.

aplicar el cumplimiento del principio de información del artículo 5 de la LOPD que es garantía asimismo de la calidad de la información, con los graves perjuicios que de ello se derivan, como errores *in personam*. No obstante, la LOPD obliga a notificar a los interesados en el plazo de 30 días desde el registro y establece en el artículo 29.4 un límite temporal *retroactivo* máximo de 6 años para el registro y cesión de los datos «adversos», entendiendo que estos comprenden no sólo el registro de las insolvencias actualizadas sino también las de «*saldo 0*» o nulo que hacen referencia a deudas ya canceladas, habiendo sido objeto de sanción por parte de la AEPD[5] ya que no se consideran un dato neutro. Distinto es que la entidad bancaria comunicante conserve los datos para su uso propio o interno derivado de la relación entidad–cliente.

En este sentido, las entidades bancarias también han sido objeto de sanción por comunicar datos erróneos a la Central de Información de Riesgos (CIRBE) del Banco de España, que no obstante, no es un fichero de carácter privado de los regulados en el artículo 29 de la LOPD, sino un «fichero de carácter público», que no es lo mismo que decir un fichero sin restricciones en el acceso.

En el ámbito sanitario, el artículo 14 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE núm. 274, de 15.11.2002), obliga a la administración sanitaria a establecer mecanismos que garanticen la autenticidad e integridad del contenido de la historia clínica y de los cambios operados en ella, lo que exige que los datos se encuentren ordenados[6] y sean completos, amén de la obligación de centralizar todos los datos en un único archivo, dada la implicación que puede suponer para el derecho fundamental a la vida y a recibir una asistencia sanitaria adecuada.

II.1.3. El principio de prohibición de exceso

Sobre el principio de prohibición de exceso, la LOPD dice que los datos deben ser no excesivos con relación al ámbito y la finalidad del fichero, de tal manera que cualquier dato no adecuado para una finalidad será siempre excesivo, pero también un tratamiento adecuado de datos puede ser excesivo por acumulación, que habrá de ser enjuiciado en el caso de cada fichero teniendo en cuenta el principio de proporcionalidad.

A este respecto podemos aplicar la doctrina contenida en la STC 207/1996 de 16.12.1996 (Sala Primera, recurso de amparo 1.789/1996, ponente José Vicente GIMENO SENDRA) «para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

A mayor abundamiento, habrá que verificar si no hay otro medio menos intrusivo

[5] Agencia Española de Protección de Datos. En adelante: AEPD.

[6] Véase artículo 17.3 de la Ley 41/2002 de 14 de noviembre, *cit.*

que permita alcanzar igualmente el fin que este tratamiento de datos –biométricos, de video vigilancia, de RFID– persigue, de manera que se supere el juicio de necesidad, además de realizar un juicio de necesidad para comprobar si el bien constitucional a alcanzar es mayor y merece la intromisión en el derecho a la protección de datos personales, algo que está acreditado, por ejemplo, en el tratamiento de datos biométricos, para garantizar la presencia de los funcionarios o empleados públicos cuando hay un problema de presencia, no así en el caso del control de asistencia de menores a centros escolares, como veremos más adelante.[7]

En cuanto a la tramitación de procedimientos administrativos por las Administraciones Públicas, hay que destacar que en virtud del principio de legalidad sólo deben solicitar los datos que estén previstos legalmente, para lo que en opinión de TRONCOSO REIGADA[8], se hace necesaria una revisión de los impresos o formularios de recogida de datos, no pudiendo utilizarse dichos datos para otras finalidades distintas para las que fueron recogidos, debiendo mencionarse en la propia leyenda del impreso, así como figurar en la tipología de datos establecida en la declaración de inscripción del fichero, donde ha debido ser declarada ya adecuada y no excesiva. No obstante, el tratamiento de datos personales dentro de la misma tipología no obliga a una modificación de la disposición de carácter general. Asimismo, el principio de finalidad impide emplear los datos para una finalidad incompatible con la que fueron recogidos, así como tampoco es posible la utilización de los datos para otro expediente por otra dependencia o servicio dentro de la misma Administración.

En este sentido, la APDCM[9] en su Resolución E/051/2006 de 17 de agosto, sancionó a la Consejería de Educación de la Comunidad de Madrid por incumplimiento del principio de calidad, al utilizar información personal que los profesores habían entregado para la concesión de un complemento retributivo para otros fines, por la recogida y tratamiento excesiva de datos y por no cancelar la publicación de la información en el momento oportuno.

Lo que sí se encuentra permitido es utilizarlos para una finalidad distinta siempre que se encuentre entre las competencias del mismo órgano administrativo, previa declaración *ex novo* del fichero y cumplimiento del principio de información, sin ser necesario el consentimiento del interesado cuando no lo fue en la primera ocasión. También se encuentra permitida la utilización de los ficheros para fines históricos, estadísticos o científicos a tenor del artículo 4.2 de la LOPD, especialmente en la labor investigadora oficial de las Universidades, siempre dentro de un proyecto institucional, previa disociación de la información personal y con la autorización previa del responsable del fichero.

Aparte, se exige la existencia de competencia administrativa y de una función que requiera la recogida de datos para una finalidad y el cumplimiento del principio de información, ya mencionado, estableciéndose en este sentido la recogida de datos de forma

[7] Véase el apartado III.6., «Principio de calidad del dato en la utilización de datos biométricos para el control del acceso de alumnos menores a centros escolares».

[8] TRONCOSO REIGADA, A., «Principios de la protección de datos: el principio de calidad de los datos» (IIª parte), *cit.*, pág. 5.

[9] Agencia de Protección de Datos de la Comunidad de Madrid. En adelante: APDCM.

engañosa o fraudulenta, como infracción muy grave en el artículo 44.4 h) de la LOPD, exigiendo la conducta dolosa del ánimo de engañar, a decir de TRONCOSO REIGADA.[10]

En cuanto al acceso, en el ámbito administrativo hay que destacar que no todo subordinado del responsable del fichero se encuentra legitimado para el acceso a los datos, sino aquellos que desempeñen el ejercicio de unas funciones relacionadas con la finalidad del fichero y que figuren en el documento de seguridad. A este respecto, en los ficheros de acceso centralizado –como historias clínicas electrónicas o expedientes académicos electrónicos– es importante establecer diferentes niveles de acceso, dependiendo de las funciones que desempeñe cada empleado, y no un acceso general a la información

En cuanto al ámbito sanitario, la información clínica debe archivarse de forma separada a la documentación administrativa o económica, de forma que el personal de administración y servicios no tenga acceso a la primera.[11]

Discutible es si el nivel político tiene acceso o no a los ficheros existentes bajo el ámbito de su responsabilidad, toda vez que en la gran mayoría de ocasiones él mismo es el responsable de los mismos. En este sentido, parece razonable que se permita el acceso cuando sea necesario para el desempeño de su cargo, ya que va a responder políticamente de la gestión desempeñada en su área de gobierno.

Por otro lado, el principio de calidad obliga a que los datos personales se registren sin errores, por lo que es preferible que cuando esto sea posible, la obtención se realice a través del propio interesado y con la menor intrusión –respetando los principios de lealtad y licitud–, y siempre debe evitarse el tratamiento por parte de terceros que puede suponer una cesión no consentida o el incumplimiento del deber de secreto.

Como ejemplo, un Ayuntamiento que tramite un procedimiento sancionador en materia de tráfico debe mantener actualizados los datos del domicilio fiscal del interesado[12], que pueden diferir de los obrantes en el padrón municipal, de tal forma que en la tramitación del procedimiento de apremio en caso de impago –sobre todo en la fase de notificación–, no se vean afectados los derechos del apremiado, y especialmente su derecho de defensa, lo que podría conllevar la anulación de todo el procedimiento en vía contencioso–administrativa.

A este respecto, la Corporación tiene la obligación tanto de mantener actualizadas sus propias bases de datos *alimentándolas* con los datos del Registro de vehículos que la Dirección General de Tráfico pone a su disposición, como el Padrón Municipal, en virtud de los artículos 17 y 60 a 92 del Real Decreto 1690/1986, de 11 de julio, que aprueba el Reglamento de Población y Demarcación de las Entidades Locales (BOE núm. 194, de 14.08.1986; en adelante: RPDEL).

Asimismo, debe mantener actualizado y conservar los datos del fichero de Recaudación Ejecutiva, no solamente para la tramitación de los procedimientos de apremio, sino para emitir los correspondientes certificados, a solicitud del interesado, de los pagos

[10] TRONCOSO REIGADA, A., «Principios de la protección de datos: el principio de calidad de los datos» (IIª parte), *cit.*, pág. 6.

[11] Véase artículo 16 de la Ley 41/2002 de 14 de noviembre, *cit.*

[12] A este respecto pueden consultarse los apartados IV.6. y IV.7. de este trabajo, donde se estudian dos Resoluciones de la APDCM sobre el tema.

efectuados.[13]

A mayor abundamiento, hay disposiciones de carácter general de muy diversa índole y procedencia que no respetan el principio de calidad al exigir datos que no están previstos en la normativa aplicable o son excesivos en relación con la finalidad, por lo que son susceptibles de ser impugnados mediante los recursos pertinentes.

Esta exigencia se hace más evidente en la tramitación electrónica de procedimientos administrativos mediante los instrumentos de la sociedad de la información, por lo que el artículo 4 g) de la LAESP dice que sólo se requerirá a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten, en relación con el artículo 35 f) de la Ley 30/1992 de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (BOE núm. 285, de 27.11.2002; en adelante: LRJPAC), que establece el derecho de los ciudadanos a no presentar documentos no exigidos por las normas del procedimiento de que se trate o que se encuentren en poder de la Administración actuante. Además, el artículo 10.2 del mismo cuerpo legal señala que el establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto a la integridad, veracidad y actualización de la información y de los servicios a los que pueda accederse a través de la misma, según menciona TRONCOSO REIGADA.[14]

Por su parte, cuando se detecte la inexactitud de los datos recogidos en una solicitud de un servicio de administración electrónica, se debe proceder a la corrección de los mismos, así como a comunicar a otras Administraciones, a las que se hayan cedido los datos, cuantas incorrecciones se hayan podido observar.

Especialmente protegidos se encuentran los datos relativos a la ideología, religión o creencias, raza, salud o vida sexual[15], y por lo tanto deben ser analizados con mayor dedicación por su predisposición a esconder tratamientos inadecuados o excesivos, como lo es por ejemplo el tratamiento de los datos del diagnóstico médico de un funcionario para evaluar las retribuciones que le corresponden por productividad, no así el tratamiento de datos biométricos de los trabajadores por el empresario con la única finalidad del control de accesos cuando no exista un medio menos intrusivo.

Dicho esto, la LOPD prevé una excepción en el artículo 7.6 para el tratamiento de los mismos con objeto de la prevención, el diagnóstico clínico, la asistencia sanitaria y la gestión del propio servicio por parte de los servicios sanitarios, así como de la historia social en el caso de los trabajadores sociales, que comprende un elenco de características íntimas del propio sujeto y de su entorno social, por lo que sería deseable el establecimiento de unos criterios orientativos comunes. También se encuentra permitido el acceso a la historia clínica con fines epidemiológicos, de salud pública, de investigación o docencia, si bien se exige la previa disociación de los datos personales del paciente para garantizar el anonimato.[16]

[13] Véase artículo 32 del Real Decreto 1684/1990 de 20 de diciembre, que aprueba el Reglamento General de Recaudación.

[14] TRONCOSO REIGADA, A., «Principios de la protección de datos: el principio de calidad de los datos» (Iª parte), *cit.*, pág. 15.

[15] Véase artículo 7 de la LOPD.

[16] Véase artículo 16.3 de la Ley 41/2002 de 14 de noviembre, *cit.*

La recogida de datos ha de ser por lo tanto leal y lícita, prohibiendo la LOPD el tratamiento de datos ilícitos o desleales, y siempre debe ser transparente, no siendo legítimos los tratamientos ocultos.

En cuanto al almacenamiento de los datos, debe hacerse de forma que permita el derecho de acceso según el artículo 4.6 de la LOPD, ya que es condición necesaria para permitir el ejercicio de otros derechos como el de rectificación, oposición y cancelación.

En este sentido, la LAECSP obliga a las Administraciones Públicas a la conservación en formato electrónico de los documentos electrónicos que formen parte de un expediente[17], debiendo realizarse siempre que sea posible de forma centralizada, lo que favorece la seguridad de la información y evita, por ejemplo, la repetición de pruebas en el ámbito sanitario, con el consiguiente ahorro económico para las arcas públicas.

En cuanto a la conservación de ficheros en el ámbito sanitario, la Ley 41/2002 establece un plazo mínimo de 5 años desde la fecha de alta de cada asistencia[18], que deberá modularse dependiendo de cada caso concreto, y siempre realizarse con las debidas condiciones de mantenimiento y seguridad.

En el ámbito educativo no universitario, se prevé la conservación del expediente académico que no puede cancelarse aunque haya finalizado el período académico, no así los cuadernos de tutoría o la documentación de intervención psicopedagógica.

II.2. El principio de calidad del dato en la Administración Local

En primer lugar, tal y como dispone el artículo 4.2 de la LOPD, los datos recabados por la Corporación no podrán ser utilizados para finalidades incompatibles con aquellas para las que los datos hubieren sido recogidos.

En este sentido, cabe destacar que la Administración actuante ostenta personalidad jurídica única en sus relaciones externas, a la hora de ejercitar competencias y de ser sujeto de obligaciones y responsabilidades.

En el caso de las Administraciones Públicas, la creación de ficheros debe realizarse mediante una disposición general que especifique la finalidad, contenido y uso del mismo, así como determine la autoridad responsable del tratamiento y del fichero, aparte de la obligación legal de inscripción del mismo –con carácter general– en el registro existente al efecto en la AEPD o equivalente autonómico, en su caso.

En el supuesto concreto de una Corporación Municipal, sólo a través del Pleno pueden crearse ficheros nuevos y será este el responsable del mismo así como del tratamiento de los datos personales, sin perjuicio del ejercicio de la potestad de auto–organización interna mediante la cual puede ser encomendada esta función a otros órganos de la misma.

A mayor abundamiento, dicho tratamiento debe estar en consonancia con las competencias que dicho órgano tenga atribuidas y deben figurar las personas autorizadas a acceder a cada fichero en particular, tal y como dispone el Real Decreto 994/1999 de 11 de

[17] Véase artículo 6.2 f) de la LAECSP, *cit.*

[18] Véase artículo 17.

junio (BOE núm. 151, de 25.06.1999; en adelante: RMSFA).

En concreto, en el ámbito de las notificaciones que deba efectuar la Corporación Municipal en relación con la gestión catastral, la propia normativa urbanística obliga a notificar a los titulares que obren en el Catastro –piénsese también en la gestión del IBI–, y por lo tanto será necesario conocer el dato del domicilio de los mismos, que podrá obrar a su vez en el Padrón de habitantes del municipio o no, dependiendo de si el titular tiene la vecindad en dicho término municipal.

Dicha cesión de datos fue objeto de análisis en el Informe jurídico de la AEPD número 171/2003, como veremos más adelante.

II.2.1. Especial referencia al Padrón de habitantes

Tras una preliminar y fugaz consulta de la legislación básica reguladora del régimen local, no resulta complicado deducir que el Padrón municipal de habitantes constituye la principal y más importante fuente de información de datos de carácter personal con que cuentan los municipios españoles. Pero su trascendencia va más allá y rebasa los límites del término municipal para adentrarse en el ámbito de otras Administraciones de carácter supramunicipal, siendo de referencia para la prestación de asistencia sanitaria no urgente o para el acceso a determinadas ayudas sociales de carácter autonómico, por ejemplo, y sin tener en cuenta todo el elenco de funciones estadísticas a nivel autonómico, estatal y comunitario.[19]

Debido a la importancia de dicho Registro, se hace necesario analizar la aplicación sobre el mismo de la legislación estatal de protección de datos en relación con el principio de calidad de los datos, si bien, la finalidad y configuración legal del Padrón municipal excede del régimen estricto de inscripción en la AEPD o Agencias autonómicas aplicable a otros Ficheros.

En primer lugar, la Corporación municipal deberá respetar lo dispuesto en el artículo 4.3 de la LOPD, en el sentido de la obligación de mantener los datos de los interesados obrantes en el Padrón continuamente actualizados, de manera que figuren exactos y veraces.

En segundo lugar, deberá cumplir igualmente lo dispuesto en el artículo 4.2 del mismo cuerpo legal en el sentido de no poder emplear, sin consentimiento del afectado, dichos datos para finalidades distintas para las que fueron recabados. Dicha obligación lo es no solamente en relación con otras Administraciones públicas o terceros, sino también en relación con el propio municipio responsable del Fichero.

En este sentido, las funciones primordiales del Padrón fueron definidas por los artículos 15 y 16 de la LBRL, y son por una parte la de determinar cualitativamente la condición de vecino del municipio, y por otra la de determinar cuantitativamente la población de dicho municipio.

No obstante, la Jurisprudencia ha venido configurando la legalidad o no de *otros usos* del Padrón, que obviamente pueden ser tan variados que no cabe establecer una regla

[19] Compruébese la relación entre el artículo 17.3 de la LBRL y la función estatal de elaboración del Censo, así como la determinación de cifras oficiales y de estadísticas nacionales y comunitarias.

general; así, la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 21 de abril de 2004 (sección primera, Roj: SAN 2741/2004, ponente Fernando F. Benito Moreno) entra a conocer sobre el posible incumplimiento de la legalidad por parte del Alcalde de Sabadell al remitir unas cartas a los vecinos del municipio nacidos en Lorca (Murcia) tras realizar una visita por invitación de su Alcalde, localidad con la que se había formalizado un hermanamiento. La Sala entendió, paradójicamente, que dicho uso del Padrón era ajustado a Derecho, considerándolo como Registro de Población del Municipio a efectos de comunicación entre Administración local y vecinos.

Por su parte, la Sentencia del TSJ de Madrid de 11 de enero de 2006 (sección octava, Roj: STSJ MAD 3553/2006, ponente: Inés María HUERTA GARICANO) revoca la dictada por el Juzgado de lo Contencioso-Administrativo confirmatoria de la Resolución sancionadora impuesta por la Agencia de Protección de Datos de la Comunidad de Madrid al Ayuntamiento de Las Rozas, al haber usado su Alcalde los datos obrantes en el Padrón para enviar las felicitaciones navideñas. El argumento utilizado por la Sala es que el Padrón se encuentra a disposición del Alcalde para el desempeño de las funciones municipales, encontrándose entre dichas funciones la relación de éste con los vecinos.

En tercer lugar, en cuanto a la utilización del Padrón por otros órganos del Ayuntamiento diferentes a los responsables del fichero y a los encargados del tratamiento, hay que destacar que no nos encontramos ante un supuesto de cesión de datos –toda vez que el acceso se realiza desde la propia Administración–, y habrá que valorar si la finalidad es o no compatible con la que propició la recogida de los datos, por ejemplo será válida si el acceso se lleva a cabo para recabar los datos de identidad y/o domicilio para llevar a cabo sus competencias.

Como ya sabemos, todo tratamiento de datos personales ha de ser adecuado, pertinente y no excesivo con la finalidad del mismo, por lo que todo acceso indiscriminado constituiría una violación del derecho a la protección de datos determinante de la nulidad de las actuaciones del órgano administrativo.

Para que dicho acceso sea ajustado a Derecho y no derive en la nulidad de actuaciones, debe ser llevado a cabo dentro de las competencias del órgano actuante y siempre debe ser compatible con la finalidad primaria del Padrón, toda vez que la exención de recabar el consentimiento del interesado sólo abarca a esta última.

Todo acceso deberá ser restringido a los datos estrictamente necesarios para el ejercicio de la competencia, siempre que los mismos sean imprescindibles para dicho ejercicio, respetándose la confidencialidad y garantizando la seguridad de los datos en toda la cadena de custodia.

II.2.1.1. Utilización del Padrón por los Concejales

En primer lugar, hay que hacer una distinción entre Concejales que desempeñen funciones de gobierno y aquellos que no se encuentren en este supuesto.

Los primeros pueden hacer un uso legítimo de los datos personales obrantes en el Padrón Municipal en el ejercicio de sus competencias y siempre que dicho uso sea compatible con su función originaria, al igual que los órganos municipales como ya se ha dicho.

Más complejo es calificar dicho uso por los Concejales de la oposición. A este respecto, el TSJ de Madrid se pronunció en su Sentencia de 13 de junio de 2001 (sección octava, Roj: STSJ MAD 8001/2001, ponente: Inés María HUERTA GARICANO) levantando la sanción impuesta por la AEPD al Grupo Municipal del Partido Popular del Ayuntamiento de Leganés, por utilizar los datos obrantes en el Censo Electoral –obsérvese que no se trata del Padrón– para informar a los vecinos de la apertura de una Oficina de Atención al Ciudadano por dicho Grupo Municipal.

El TSJ entiende que dicho uso queda amparado porque tanto el Padrón como el Censo son instrumentos de comunicación con los vecinos y el electorado, respectivamente, a quienes representan los Concejales, y que dicha utilización lo fue para ofrecerles un servicio en el ejercicio de sus funciones.

A mayor abundamiento, se hace necesario conciliar el derecho del individuo a la protección de datos personales con la función pública que tienen asignada los Concejales, por lo que es irrelevante, a efectos sancionadores, que dichos datos sean obtenidos del Censo electoral o del Padrón de habitantes.

El amparo legal de dicha intervención lo otorga el artículo 77 de la LBRL, ya que permite obtener del Alcalde o Presidente o de la Comisión de Gobierno cuantos antecedentes obren en poder de los servicios de la Corporación y sean necesarios para el ejercicio de sus funciones, en concreto, de control como oposición de la actividad política.

Dicho esto, los Concejales deberán respetar el deber de secreto respecto a los datos personales que conozcan en el desempeño de sus cargos, así como especialmente el principio de calidad de los datos, en el sentido de que estos sean tratados de forma adecuada y pertinente, y el uso que de los mismos se haga no sea incompatible con la función originaria del fichero para el que fueron recabados, a decir de FUENTETAJA PASTOR y MEDINA GONZÁLEZ.[20]

II.2.1.2. Uso del Padrón por la Policía Municipal

En principio, la utilización que pueda hacer la Policía Municipal de los datos obrantes en el Padrón, sigue el mismo patrón que el del acceso por otros órganos de la Administración Local ya analizado anteriormente, es decir, se trata de un acceso derivado.

No obstante, el artículo 22 de la LOPD engloba a este cuerpo junto con las Fuerzas y Cuerpos de Seguridad del Estado, por lo que el uso de los mismos deberá limitarse a la prevención de un peligro real para la seguridad pública, así como a la represión de infracciones penales.

Mayor complejidad presenta el uso de los datos calificados como de «especialmente protegidos» –a que hace referencia el artículo 7.3–, por ejemplo del lugar de nacimiento o de nacionalidad del sujeto, de los que cabe fácilmente deducir su origen racial. En este supuesto, dicha utilización se encuentra legitimada estrictamente en el curso de una investigación concreta, sin perjuicio del control judicial y de legalidad de las actuaciones, tal

[20] FUENTETAJA PASTOR, J. y MEDINA GONZÁLEZ, S., *La Protección de Datos en la Administración Local*, Iª edición, Madrid, Iustel, 2008, Págs. 144 y ss.

y como lo mencionan FUENTETAJA PASTOR y MEDINA GONZÁLEZ.[21]

II.2.2.1. Uso de ficheros municipales por organismos o empresas públicas

Como bien sabemos, cuantas más competencias ostenta y mayor en tamaño es una Administración pública, más compleja se vuelve su estructura y sus órganos se encuentran más especializados, en virtud del principio de descentralización administrativa.

Toda esta dinámica conlleva la creación de organismos públicos de la más diversa índole –organismos autónomos, entidades públicas empresariales, agencias– a los que se unen las empresas o sociedades del sector público –con personalidad jurídica privada y una participación pública de al menos el 50%– y las fundaciones en sus diferentes modalidades.

A mayor abundamiento, la configuración legal de cada uno de dichos organismos –que daría para varios trabajos jurídicos– varía según el tipo de Administración ante la que nos encontremos –Estatal, Autonómica, Local e incluso Institucional–, por lo que se hace necesario establecer brevemente un punto común de referencia en cuanto al régimen de la utilización de los datos personales obrantes en los ficheros de la Administración matriz.

A este respecto, hay que destacar que si el organismo o empresa pública ostenta una personalidad jurídica propia y diferenciada de la Administración matriz, la utilización de los datos personales provenientes de la Administración matriz es considerada una comunicación o cesión de datos a otra Administración diferente, y por lo tanto son de aplicación las reglas previstas en la legislación de protección de datos a estos fines.

En el caso concreto de las Corporaciones locales, el uso del Padrón por estos organismos o empresas públicas, en cuanto al régimen de la protección de datos, es considerado de igual modo, pero como es sabido, dicho uso deberá hacerse en el ejercicio de una competencia y ser proporcional a los fines que se pretenden y siempre que éstos sean compatibles con la finalidad originaria del fichero, amén del respeto al principio de calidad de los datos y demás principios de la protección de datos.

II.2.2. Uso de ficheros municipales por personas jurídico-privadas del Sector público local

Dentro de las personificaciones jurídico–privadas del sector público municipal encontramos las empresas o sociedades privadas pertenecientes al sector público local –con al menos una participación municipal del 50%– y las fundaciones *privadas* municipales, sin perjuicio de la existencia de otros entes *privados*.

En este caso, la utilización de datos personales recabados por la Corporación municipal no puede ser considerada una cesión de datos a otra Administración, toda vez que la personalidad de estos entes es privada, por lo que no son considerados Administración propiamente dicha, si bien se encuentran en la esfera del Sector Público

[21] FUENTETAJA PASTOR, J. y MEDINA GONZÁLEZ, S., *La Protección de Datos en la Administración Local, cit.*, págs. 147 y 158.

local, según disponen en su obra FUENTETAJA PASTOR y MEDINA GONZÁLEZ.[22]

Por lo tanto, el régimen de protección de datos aplicable a estas transacciones de datos es el relativo a la cesión de datos personales de una Administración pública a terceros, por lo que no es de aplicación lo establecido en el artículo 21 de la LOPD, en este caso.

III. Análisis de algunos Informes de la AEPD relativos a la aplicación del principio de calidad de los datos

III.1. Principio de calidad del dato y acceso al Registro de Vehículos.

El Informe 184/2006 hace referencia a la utilización de los datos del Registro de Vehículos para fines distintos a los legítimos de acceso al mismo en relación con los artículos 4.1 y 4.2 de la LOPD.

En concreto, un periodista obtuvo del Registro de Vehículos, fuera de su ámbito laboral, los datos referidos al vehículo del que es titular un cargo público y los facilitó a un tercero, no identificado, para su difusión en forma de fotocopias repartidas en distintas dependencias administrativas de la Comunidad Autónoma así como en los parabrisas de los vehículos que se encontraban en las proximidades de la sede de las mismas.

Por su parte, el párrafo tercero del artículo 2 del Real Decreto 2822/1998, de 23 de diciembre, por el que se aprueba el Reglamento General de Vehículos (BOE núm. 22, de 26.01.1999), establece el carácter público de dicho Registro, así como regula el acceso por parte de los interesados y aquellos que tengan un interés legitimo y directo, aun sin contar con el consentimiento del afectado.

A mayor abundamiento, el concepto de interesado empleado en dicho Reglamento no es equiparable al concepto legal establecido en el artículo 31 de la LRJPAC, correspondiendo a la Dirección General de Trafico la apreciación de dicho interés.

En conclusión, la AEPD estima que dicha actuación es contraria a la LOPD en tanto los datos han sido obtenidos con la finalidad de ser divulgados masivamente y no para los fines permitidos por la normativa reguladora del mismo, toda vez que el artículo 4.2 prohíbe la utilización de dichos datos para finalidades distintas para las que fueron obtenidos.

III.2. El principio de calidad del dato y su relación con el plazo de conservación

El Informe 408/2010 responde a una consulta sobre el plazo de conservación de los datos personales de los clientes, así como sobre el plazo en que puede procederse a su destrucción, en cumplimiento de lo preceptuado en el artículo 4.5 de la LOPD y 8.6 del Reglamento.

Hay que señalar que la cancelación de los datos no supone su supresión automática, sino que debe bloquearse su acceso tal y como dispone el artículo 16.3 de la LOPD,

[22] FUENTETAJA PASTOR, J. y MEDINA GONZÁLEZ, S., *La Protección de Datos en la Administración Local, cit.*, pág. 84.

quedando a disposición de las Administraciones públicas, Jueces y Tribunales durante el tiempo de prescripción de las hipotéticas responsabilidades en que hubieren podido incurrir, pudiendo proceder a su supresión una vez transcurrido este plazo.

Dicho bloqueo debe efectuarse de forma que no sea posible el acceso por el personal que habitualmente tuviera acceso a los mismos, pudiendo efectuarse exclusivamente por una persona con la máxima responsabilidad y en virtud de requerimiento judicial o administrativo a tal efecto.

El Informe indica que no puede establecerse un periodo concreto valido para todos los casos, pero añade que según Informe de 1 de agosto de 2005 además de la relación entre responsable e interesado a que hace referencia el artículo 16.5 de la LOPD, habrá que estar a las disposiciones aplicables y a las responsabilidades nacidas del tratamiento, como ya se apuntó.

A mayor abundamiento, la STC 292/2000 de 30 de noviembre (pleno, recurso de inconstitucionalidad 1463-2000, ponente: Julio Diego GONZÁLEZ CAMPOS) dice que para que el bloque se considere lícitamente efectuado deberá constar en un disposición con rango de Ley, como por ejemplo, el plazo de 4 años establecido en la Ley de Derechos y Garantías de los Contribuyentes para la prescripción de la deuda tributaria en relación con la obligación de conservación establecida en el artículo 111 de la Ley General Tributaria.

En último lugar, cabe añadir el plazo de prescripción de 3 años que establece el artículo 47.1 de la LOPD para las conductas tipificadas como muy graves, a salvo otros plazos establecidos en normativa sectorial con rango de Ley.

III.3. Principio de calidad del dato y control electrónico de los trabajadores

El Informe 615/2009 entra a conocer de la adecuación a la normativa de Protección de Datos de un Reglamento de uso de los medios informáticos propios de un Ayuntamiento por parte de sus empleados, como el correo electrónico y el acceso a Internet, y trata de responder a la consulta planteada a estos efectos por el Comité de Empresa.

En este sentido, señala el Informe que los trabajadores y sus representantes deberán ser informados de los medios utilizados por el empresario para vigilar su actividad laboral, no pudiendo recabar datos que se consideren excesivos.

A mayor abundamiento, los representantes de los trabajadores deberán estar informados de todo nuevo sistema que se instale en este sentido y tendrán acceso a los datos que se procesen sobre ellos, así como podrán ejercitar el derecho de rectificación.

En cuanto al derecho de información, el trabajador tendrá acceso a los datos recabados excepto cuando se tengan fundadas sospechas de que se encuentre realizando alguna actividad delictiva o dolosa, con el objeto de poder rebatirla.

Por su parte, el Grupo de Trabajo del articulo 29 emitió Dictamen 8/2001 indicando que en el devenir de la vida diaria del trabajador, multitud de datos resultan recogidos por parte del empleador, ya sea a través de las nuevas tecnologías de la información y las comunicaciones o a través de los sistemas de video vigilancia, que también se encuentran sometidos a la Legislación sobre Protección de Datos.

Dicho control deberá hacerse respetando, en todo caso, el derecho a la vida privada y

otros intereses de los trabajadores.

Mayor problema presentan los sistemas de supervisión del correo electrónico entrante y saliente, toda vez que es factible someter a vigilancia el correo corporativo saliente de los trabajadores, previa información a los mismos, si es posible solamente respecto al tráfico, las horas del mismo, el formato de los archivos adjuntos y el número de mensajes enviados o recibidos, obviando por lo tanto el contenido. En cuanto al correo entrante, no es posible efectuar dicha comunicación de antemano en todos los casos, pero una posible solución sería avisar en los correos salientes de tal extremo.

También puede adoptar otras medidas más eficaces –que deberán ser siempre proporcionadas– como el bloqueo previo del acceso a determinados sitios web de la red de redes, o la instalación de medidas de aviso automáticas, así como mediante sistemas estadísticos.

A este respecto, el Grupo de Trabajo del artículo 29 emitió el Documento de Trabajo de fecha 29 de mayo de 2002, sobre la vigilancia a que hemos hecho referencia tanto en tiempo real como sobre los datos almacenados. Así, respecto al principio de proporcionalidad, los datos personales que se recaben deberán ser adecuados, pertinentes y no excesivos para los fines a los que se destinen, y deberá adaptarse al tipo y grado de riesgo de la empresa. Por lo tanto, debe evitarse un sistema generalizado de vigilancia electrónica y optar por el mas proporcionado, evitando los sistemas que efectúan una vigilancia automática y continua.

Sobre la conservación de los datos de tráfico en Internet y del uso de correo electrónico, el Documento dice que deberá adaptarse a las circunstancias de cada empresa, pero que generalmente no debe exceder de 3 meses, además de ser precisos y encontrarse actualizados.

En cuanto a la seguridad, el empleador debe adoptar las medidas necesarias para proteger los sistemas de cualquier ataque o virus informático, lo que puede conllevar el análisis automático de todos los mensajes entrantes y salientes, así como del tráfico de Internet.

Todas las tareas mencionadas han de recaer en el administrador del sistema, que adquiere la responsabilidad sobre la adopción de las medidas exigidas por la Ley y se encuentra sometido al secreto profesional.

En cuanto a la actividad de las Administraciones Públicas, el artículo 1.2 de la LAECSP dispone que estas deberán velar por el aseguramiento de la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias, ya sea entre sí mismas o en sus relaciones con los ciudadanos.

El artículo 42.2 del mismo texto legal crea el Esquema Nacional de Seguridad, cuya función es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Dicho Esquema Nacional es desarrollado mediante Real Decreto 3/2010, de 8 de enero, cuya exposición de motivos dice que se crea un común denominador normativo que podrá ser completado, mediante objetivos, materialmente no básicos que podrán ser decididos por políticas legislativas territoriales, por lo que todos los órganos superiores de las diferentes Administraciones deben disponer de una política de seguridad electrónica que deberá ser aprobada por el titular de dicho órgano superior.

Por su parte, los municipios podrán disponer de una política común de seguridad elaborada por la Diputación, Cabildo, Consejo u órgano provincial equivalente o bien por la entidad comarcal correspondiente.

El artículo 14 del Real Decreto hace referencia a la seguridad en el acceso del personal y a su formación, estableciendo la obligatoriedad de su información en cuanto a deberes y obligaciones, así como a la supervisión en cuanto al cumplimiento de los procedimientos.

El artículo 23 del mismo texto normativo establece expresamente la retención de datos de los usuarios con plena identificación de los mismos, para evitar un uso indebido o fraudulento, con plenas garantías del derecho al honor, a la intimidad personal y familiar, y a la propia imagen de los afectados.

En cuanto a la proporcionalidad de las medidas, la STC 207/1996 (Sala Primera, recurso 1789-1996, ponente Vicente GIMENO SENDRA) establece tres medidas para verificar que una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, a saber:

1.- Juicio de idoneidad: Si tal medida es susceptible de conseguir el objetivo propuesto.

2.- Juicio de necesidad: Si es necesaria por no existir otra medida menos lesiva con igual grado de eficacia.

3.- Juicio de proporcionalidad en sentido estricto: Si la misma es ponderada o equilibrada por derivarse de ella más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Finalmente, destacar de este Informe que las competencias sobre protección del derecho a la intimidad o del secreto de las comunicaciones no corresponden a la AEPD.

III.4. Principio de calidad del dato en la auditoría informática de una Administración

El Informe 417/2009 analiza la interesante y compleja cuestión del alcance que puede tener una auditoría informática realizada por el Administrador de Red de un Organismo Público sobre un servidor dividido en varias Unidades de Red, disponiendo cada empleado de una unidad propia de acceso exclusivo y que fue entregado al director del centro.

Sobre las actuaciones dentro del ámbito de competencias de la AEPD, ésta realiza un análisis previo de su competencia para conocer del asunto, verificando que el listado con el nombre de los archivos con su extensión del servidor asociado a los empleados pueda contener datos personales, especialmente en cuanto a la legitimidad y en lo que pueda afectar al principio de calidad de los datos en sus vertientes de finalidad y proporcionalidad

del tratamiento.

A este respecto, la Recomendación 1/2001 del Grupo de Trabajo del Artículo 29, establece que la utilización de ese listado con la finalidad de evaluar a los empleados podría dar lugar a su consideración como un dato personal y lo mismo si existe un elemento de resultado aun cuando no figuren los datos mencionados.

Después de hacer una sistematización de los instrumentos internacionales aplicables a la protección de datos en el ámbito laboral respecto de los trabajadores –ya referido anteriormente–, el Informe se refiere a normativa interna y especialmente en lo que interesa al Esquema Nacional de Seguridad –creado por el artículo 42.2 de la LAECSP, como ya dijimos–, y al Real Decreto 3/2010 de 8 de enero, cuyo artículo 1.2 dice:

> «El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.»

También son de aplicación al caso los artículos 11, 14 y 23 del mismo, asimismo ya mencionados *supra*.

De especial importancia es la STS de 26 de septiembre de 2007, en recurso para unificación de doctrina, referida a la obligación de informar al trabajador sobre las reglas de uso del ordenador y los controles que sobre los mismos efectuará el empresario, dentro del poder que le confiere el artículo 20.3 del Estatuto de los trabajadores.[23]

En concreto, su FJ IV en cuanto a los límites de las facultades de vigilancia y control se refiere a que deberán guardar en su adopción y aplicación la consideración debida a la dignidad del trabajador, así como respetar el derecho a la intimidad de los mismos, tal y como establecen las STC 98 y 186/2000, entre otras.

Como ya dijimos, lo que debe hacer el empresario es informar previamente a los trabajadores de las reglas de uso de los medios informáticos, con sus prohibiciones absolutas y parciales, así como de los medios de control que se van a emplear y otras medidas, en su caso, especialmente en relación con el uso de Internet y del correo electrónico, así como de la posibilidad de recibir mensajes privados o descargar contenidos multimedia en el propio ordenador o servidor corporativo.

A este respecto, es interesante la configuración que del concepto de «expectativa razonable de intimidad» hacen las Sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997[24] y de 3 de abril de 2007[25] en relación con el artículo 8 del CEDH.

En cuanto al cumplimiento del principio de calidad de los datos y de proporcionalidad en el control, viene dada por la necesidad de garantizar la seguridad de los sistemas informáticos, contribuyendo las notas técnicas sobre volumen y limitación de utilización a especificar cuál es la finalidad del tratamiento de los datos.

[23] Véase al respecto la «Guía de protección de datos en las relaciones laborales», editada por la AEPD.

[24] Caso *Halford*.

[25] Caso *Copland*.

Para examinar la proporcionalidad del control en relación con dicha finalidad, aplicamos los tres criterios conocidos: el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad en sentido estricto.

Si dicho examen es superado, el control objeto de consulta supera las exigencias de la LOPD, si bien deberá realizarse preferentemente mediante sistemas estadísticos que generen indicadores de gestión o de uso que detecten posibles comportamientos desviados de la política de seguridad del uso de las tecnologías de la información y de las comunicaciones corporativas de la empresa u organismo público, de manera que se recojan solamente aquellos que resulten adecuados, pertinentes y no excesivos.

III.5. Naturaleza de los ficheros de las Comunidades de Regantes

En el Informe 156/2003 se analiza la naturaleza de los ficheros de las Comunidades de Regantes, y en concreto, su naturaleza pública o privada, debiendo destacar que la LOPD no establece un concepto de los mismos, por lo que habrá que estar a la naturaleza jurídico–publica o jurídico–privada de los responsables del fichero.

Dicha diferenciación no es baladí, toda vez que el artículo 21.1 de la LOPD permite la creación de ficheros derivada del ejercicio de una competencia, así como la cesión de datos entre Administraciones Publicas siempre en el ejercicio de esa misma competencia.

Por su parte, el artículo 20 del mismo cuerpo legal establece que el fichero debe estar a cargo de una Administración pública, debe crearse mediante disposición de carácter general, y en supuestos de mayor complejidad, debe ser creado como consecuencia del ejercicio de potestades públicas.

A este respecto, hay que destacar que las Comunidades de Regantes presentan un régimen mixto público-privado, llevando a cabo funciones y ejerciendo potestades de Derecho Público como Administración Corporativa por habilitación legal –véase Dictamen del Consejo de Estado de 11 de abril de 1996, Expte. 2863/1995, a la par que se rigen por el Derecho privado en sus relaciones internas Comunidad–miembros, aparte de lo que dispongan sus Estatutos y Ordenanzas. Son corporaciones de Derecho público con personalidad jurídica propia, y se encuentran bajo la tutela de la Administración. Su regulación básica se encuentra en los artículos 81 a 84 del Texto Refundido de la Ley de Aguas.[26]

A este respecto pueden verse las STS de 10 de octubre de 1973 y 14 de marzo de 1994 (Sala I), la STC 227/1988 de 29 de noviembre, STC 160/1985, de 28 de noviembre, STC 32/1991, de 14 de febrero, STS de 25 de enero de 2005 (Recurso de Casación en interés de la Ley 103/2002), STS de 26 de octubre de 2000 (Sala I) y STS de 3 de mayo de 1999 (Sala III).

A mayor abundamiento, el artículo 82.1 del TR de la Ley de Aguas señala respecto de las Comunidades de Regantes, lo siguiente:

«Tienen el carácter de corporaciones de derecho público, adscritas al Organismo de cuenca, que velará por el cumplimiento de sus estatutos u ordenanzas y por el buen orden

[26] Real Decreto Legislativo 1/2001 de 20 de julio. En adelante: TR de la Ley de Aguas.

del aprovechamiento. Actuarán conforme a los procedimientos establecidos en la presente Ley, en sus reglamentos y en sus estatutos y ordenanzas, de acuerdo con lo previsto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común».

Llegados a este punto, el Informe dispone que es de aplicación al caso la doctrina mantenida por la propia Agencia sobre la naturaleza pública o privada de los ficheros de otras corporaciones de Derecho público, como los Colegios Profesionales o las Cámaras de Comercio, en el sentido de que serán considerados en una u otra forma dependiendo de la naturaleza de las finalidades que justifiquen dicho tratamiento.

Por lo tanto, los ficheros creados con la finalidad de desarrollar las funciones de «imperium» de la Comunidad, como los referidos en los artículos 84.5, 84.6, 81.1 y 83.1 del TR de la Ley de Aguas, estarán sujetos al régimen de los ficheros públicos de la LOPD, sirviendo como ejemplo la elaboración del censo de integrantes de la misma o los relacionados con las decisiones de los jurados de riegos.

Finalmente, el resto de ficheros creados por la Comunidad que no reúnan los requisitos mencionados serán considerados ficheros privados, sirviendo como ejemplo el fichero de personal de la entidad, cuyos miembros están sujetos a una relación de tipo laboral y no de carácter estatutario.

III.6. Principio de calidad del dato en la utilización de datos biométricos para el control del acceso de alumnos menores a centros escolares

En el Informe 368/2006 se analiza la conformidad o no a Derecho de la utilización de la huella dactilar como medio de identificación de los alumnos para el acceso y salida del Colegio, así como para gestionar las ausencias y retrasos.

Sobre el régimen jurídico aplicable a los datos biométricos, la LOPD define en su artículo 3 a) los datos de carácter personal como «cualquier información concerniente a personas físicas identificadas o identificables», siendo estos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc.

Como ya sabemos, según el artículo 4.1 de la LOPD y en relación con el principio de calidad de los datos, solo podrán recabarse datos cuando los mismos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

En el caso concreto, se trata de determinar la proporcionalidad de la medida en relación con el fin pretendido, teniendo en cuenta que se trata de menores de edad. Así, según el Documento de Trabajo sobre biometría del Grupo de Trabajo del artículo 29, de 1 de agosto de 2003, dicha actuación es contraria a Derecho por excesiva y desproporcionada, en virtud de lo dispuesto en la Directiva 95/46/CE.

Finalmente, se considera dicha actuación contraria a lo dispuesto en el artículo 4.1

de la LOPD, por lo que deberá buscarse una solución menos intrusiva en relación con los derechos de los alumnos.

III.7. Principio de calidad del dato y cesión de datos entre órganos de una misma Administración

El Informe 171/2003, a que hicimos referencia anteriormente, trata el caso de la cesión de datos del padrón del Impuesto sobre Bienes Inmuebles y de las bases de datos catastrales –por razones urbanísticas– entre distintos órganos de una Corporación municipal, en aplicación de la legislación urbanística de la Región de Murcia y si dicha cesión es conforme o no a Derecho.

La Ley 1/2001, de 24 abril, de Normas Reguladoras del Suelo en la Región de Murcia (BOE núm. 243, de 10.11.2001) establece la necesidad de notificar determinados acuerdos en materia urbanística a «los titulares que consten en el catastro», por lo que *a priori* podemos presumir que existe habilitación legal para entender exceptuada dicha actuación de la exigencia de consentimiento del interesado a que hace referencia el artículo 11 de la LOPD.

Según el artículo 139 c) de la mencionada Ley, será preceptiva la notificación a los particulares cuando se produzca una modificación que no afecte a los elementos estructurales del Plan General y las Normas complementarias, por lo que resulta preceptiva dicha notificación cuando la modificación sea de iniciativa particular, entre otras.

Es decir, los órganos municipales encargados de la gestión urbanística deben tener conocimiento del dato referido a la titularidad catastral de las fincas, así como del domicilio del titular, al fin de dar cumplimiento a las previsiones legalmente establecidas.

No obstante, dicha comunicación está sujeta a dos importantes limitaciones, por un lado que sean empleados exclusivamente en los procedimientos de notificación legalmente establecidos, y por otro lado, los datos empleados no deben ser excesivos en relación con la finalidad a la que van dirigidos, amén de ser proporcionales y adecuados, en virtud de lo dispuesto en el artículo 4 de la LOPD en relación con el principio de calidad de los datos.

A mayor abundamiento, debido a la naturaleza especial de los datos de carácter tributario, su transmisión se encuentra limitada en el artículo 113.1 de la anterior Ley General Tributaria (Ley 230/1963 de 28 de diciembre, BOE núm. 313, de 31.12.1963), de aplicación a los ficheros locales por remisión del artículo 2 de la Ley Reguladora de las Haciendas Locales.

Tales datos tienen el carácter de reservados y sólo pueden ser objeto de cesión en los casos tasados a que alude el mencionado artículo[27], por lo que al no encontrarse el supuesto

[27] «a) La investigación o persecución de delitos públicos por los órganos jurisdiccionales o el Ministerio Público.

b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.

c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las Entidades Gestoras y Servicios Comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social, así como en la obtención y disfrute de prestaciones a cargo del mismo sistema.

d) La colaboración con cualesquiera otras Administraciones públicas para la lucha contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea.

e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.

planteado en la consulta en el mencionado listado, sólo podrán ser comunicados los datos imprescindibles para efectuar dicha notificación, a saber: la identificación de los titulares catastrales de las fincas y su domicilio, así como las características que permitan individualizar la finca.

IV. Análisis de algunos Informes de la Agencia de Protección de datos de la Comunidad de Madrid relativos a la aplicación del principio de calidad de los datos

IV.1. El cumplimiento del principio de calidad de los datos en la publicación de notificaciones

La Resolución de 18 de septiembre de 2009 analiza la adecuación de la notificación de una resolución, mediante publicación en boletín o tablón de edictos de un Ayuntamiento, a la normativa de protección de datos y especialmente el cumplimiento del principio de calidad de los datos (artículo 4 de la LOPD).

En concreto, la Agencia entra a conocer mediante denuncia de particular contra la Dirección General de Consumo y la Secretaría General de un Ayuntamiento por la mencionada publicación íntegra del acto administrativo –en concreto, se trata de un procedimiento sancionador– en el tablón de edictos del mismo, tras haberle sido notificado personalmente.

En primer lugar, la LRJPAC establece que una vez intentada infructuosamente la notificación, ésta se hará por medio de anuncios en el tablón de edictos del Ayuntamiento en su último domicilio, en el «Boletín Oficial del Estado», de la Comunidad Autónoma o de la Provincia, según cuál sea la Administración de la que proceda el acto a notificar, y el ámbito territorial del órgano que lo dictó (artículo 59.5), pero si el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos, se limitará a publicar en el Diario Oficial que corresponda una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para conocimiento del contenido íntegro del mencionado acto, y constancia de tal conocimiento (artículo 61), teniendo en cuenta, además, que en el caso de documentos de carácter sancionador o disciplinario, el acceso a ellos estará limitado a los propios interesados (artículo 37.3).

Por su parte, como ya sabemos, el artículo 4 de la LOPD establece que los datos

f) La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Fiscal.

g) La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de Administración Tributaria.

h) La colaboración con los Jueces y Tribunales para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa, en la que previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.

i) La colaboración con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y con la Secretaría de ambas comisiones, en el ejercicio de sus funciones respectivas.

j) La colaboración con órganos o entidades de derecho público encargados de la recaudación de recursos públicos no tributarios para la correcta identificación de los obligados al pago.

k) La colaboración con las Administraciones públicas para el desarrollo de sus funciones, previa autorización de los obligados tributarios a que se refieran los datos suministrados».

tratados deberán ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que sean recabados, además de lo dispuesto en el artículo 10 sobre la obligación de respetar el secreto profesional por parte del responsable del fichero y de cuantos intervengan, sobre los datos personales de que tengan conocimiento en el ejercicio de sus funciones.

Por lo que la solución jurídica más ajustada a Derecho sería la publicación de una breve referencia del acto administrativo objeto de la notificación, sin incluir aquellos datos que no sean estrictamente necesarios.

Examinado el expediente, consta el intento de notificación en el domicilio del interesado –por dos veces–, así como las remisiones de los anuncios de notificación al tablón de edictos del Ayuntamiento y al Boletín Oficial de la Comunidad de Madrid, siendo su contenido no la totalidad del acto administrativo, sino un extracto en el que no constan datos personales que no sean adecuados, pertinentes o no excesivos del interesado, no produciéndose tampoco vulneración del deber de secreto o sigilo ni un acceso no autorizado de terceros al contenido del expediente sancionador.

Por lo que vistos los preceptos mencionados, así como los demás de general y pertinente aplicación, el Director de la Agencia autonómica acuerda el archivo del expediente.

IV.2. El principio de calidad del dato en la publicación de datos personales en una web oficial

La Resolución de 21 de septiembre de 2009 analiza la publicación de datos personales en la página web de una dirección general de la Comunidad de Madrid, en el marco de un procedimiento de otorgamiento de un complemento autonómico por méritos individuales a profesores de las Universidades Públicas.

Como consecuencia de la instrucción del mencionado expediente, la Agencia autonómica impuso tres sanciones a la Dirección General de Universidades e Investigación de la Comunidad de Madrid por la comisión de otras tantas infracciones tipificadas como graves en el artículo 44.3 d) de la LOPD, a saber: por vulnerar el principio de calidad en la publicación de datos en la página web institucional, por no proceder a cancelar los datos publicados en la citada página, y por usar los mismos para un fin distinto.

En cuanto a la primera de las infracciones, la sanción se impuso por vulneración del principio de calidad de los datos, consistente en tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la citada Ley, por la publicación en la página web de la Dirección General de datos excesivos como son la valoración otorgada por «sexenios relativos», «proyectos de investigación» y «quinquenios».

En cuanto a la segunda, la sanción tiene por objeto castigar la conducta consistente en tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD, por haber utilizado los datos de carácter personal recabados para el procedimiento de otorgamiento del complemento autonómico por méritos para una finalidad distinta de la que motivó su recogida como es el otorgamiento de becas a estudiantes.

Asimismo, se acuerda instar a la Dirección General de Universidades e Investigación a que, o bien cree un nuevo fichero cuya finalidad exclusiva sea la gestión de la concesión del complemento autonómico por méritos individuales, o bien realice el tratamiento en el marco del fichero de datos personales «Docencia en la educación superior de Madrid», pero sin poder utilizar los datos recabados durante ese proceso para otras finalidades ligadas al ejercicio de otras competencias que correspondan a esa Dirección General.

A mayor abundamiento, se acuerda instar a dicho órgano directivo la cancelación de los datos referidos a la concesión del complemento autonómico por méritos individuales del 2005 que aparecen en su página web.

IV.3. Cumplimiento del principio de calidad del dato en la expedición del duplicado de un título académico oficial

En la Resolución de 21 de septiembre de 2009 se analiza la adecuación a la legislación de Protección de Datos de la inclusión de la causa en la expedición de un duplicado de un Título académico, y en concreto, si dicho tratamiento puede o no ser considerado excesivo en relación con el principio de calidad de los datos consagrado en el artículo 4 de la LOPD.

Vista la legislación de aplicación al caso sobre la expedición de Títulos académicos oficiales por las Universidades, en concreto: el Real Decreto 1496/1987, de 6 de noviembre, sobre obtención, expedición y homologación de títulos universitarios; la Orden de 8 de julio, del Ministerio de Educación y Ciencia, para la aplicación de los Reales Decretos 185/1985 y 1496/1987 en materia de expedición de títulos universitarios; la Orden de 24 de diciembre de 1988, del Ministerio de Educación y Ciencia para la aplicación de los Reales Decretaos 185/1985 y 1496/1987; la Resolución de 26 de junio de 1989, de la Secretaría de Estado de Universidades e Investigación; la Resolución de 14 de octubre de 1994, de la Secretaría de Estado de Universidades e Investigación, por la que se modifica la de 26 de junio de 1989; y la Orden ECI/2514/2007, de 13 de agosto, sobre expedición de títulos universitarios oficiales de Máster y Doctor, no se aprecian causas que puedan llevar a pensar en una actuación no ajustada a Derecho o disconforme con la legislación de protección de datos.

Por lo tanto, la inclusión de la causa que motivó la expedición de un duplicado de título académico, en el propio documento, no puede interpretarse como un tratamiento excesivo de datos cuando responde a una finalidad legítima, como lo es sin duda en el presente caso.

Finalmente, el Director de la Agencia autonómica acuerda sobreseer el caso, así como proceder al archivo del expediente.

IV.4. Principio de calidad del dato en la utilización de ficheros del sistema sanitario público.

En la Resolución de 23 de septiembre de 2009, la Agencia autonómica se pronuncia sobre la utilización de los datos que constan en un fichero de usuarios del sistema sanitario de un centro de salud para fines incompatibles con los que motivaron la recogida de los datos.

El conocimiento del caso por parte de la Agencia Española de Protección de Datos comienza mediante denuncia de particular contra un Centro de Salud y su médico, ya que al parecer, este utilizó datos relativos a su domicilio y número de teléfono obrantes en los ficheros de administración de dicho centro, para presentar una denuncia en Comisaría contra la madre de una paciente infantil «por insultos».

Posteriormente, tiene conocimiento la Agencia autonómica de Madrid, teniendo lugar el mismo por traslado del expediente desde la AEPD, toda vez que las competencias de sanidad fueron transferidas a la Comunidad de Madrid.

Según aparece en el Registro de Ficheros de la Agencia Española de Protección de Datos, la finalidad del fichero de usuarios del sistema sanitario del que se extrajeron los datos, es la de conocer la identidad del paciente así como sus datos personales y los relativos a facturación del servicio prestado, estado de salud, inicial y final para la identificación y asociación de datos de historia clínica, gestión actividad asistencia, financiera, docente, producciones estadísticas e investigación sanitaria.

Por lo tanto, dichos datos han sido utilizados vulnerando el principio de calidad de los datos establecido en la LOPD, por ser utilizados para finalidades distintas o incompatibles para las que se recabaron.

El Director de la Agencia de Protección de Datos de la Comunidad de Madrid declaró que la Dirección del Área de Atención Primaria había infringido lo dispuesto en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, lo que suponía una infracción tipificada como grave en el artículo 44.3 d) de la citada norma.

Asimismo se requirió a la citada Dirección para que adoptase las medidas de orden interno que impidan que en un futuro pueda producirse una nueva infracción a los principios reconocidos en la legislación de protección de datos, y para que se iniciasen las actuaciones disciplinarias que, en su caso procedan contra el médico destinado en el Centro de Salud denunciado, por haber utilizado datos personales para una finalidad incompatible y distinta de la propia de gestión de asistencia sanitaria.

IV.5. El principio de calidad del dato en el mantenimiento y custodia de las historias clínicas

En la Resolución de 28 de septiembre de 2009, la Agencia autonómica entra a conocer, por remisión de la AEPD, y se pronuncia sobre la inexistencia de documentos –cuya existencia no fue acreditada por el denunciante– que no forman parte del contenido esencial de las historias clínicas, según la Ley 41/2002, en denuncia interpuesta por particular frente a la Fundación Hospital de Alcorcón.

Dicho particular interpuso, asimismo, querella criminal frente al Doctor que le practicó la implantación de la prótesis, desestimando el Juzgado las alegaciones del mismo y archivando la denuncia, tras practicar las pruebas que consideró pertinentes.

En la denuncia interpuesta ante la Agencia, el interesado alega vulneración de la legislación sobre protección de datos en el mantenimiento, custodia y seguridad de los datos que se integran en su historia clínica, toda vez que, como alega, no consta en su

historia clínica la planificación previa a la intervención quirúrgica que padeció.

Tras la lectura del artículo 15 de la Ley 41/2002 de 14 de noviembre, antes citada, se comprueba que dentro del contenido obligatorio de la historia clínica no se encuentra el informe a que hace referencia el paciente, por quedar incluido dentro del informe de quirófano, por lo que no se está produciendo una actuación *contra lege*.

A mayor abundamiento, también el propio paciente tuvo acceso íntegro a la historia clínica, y este hecho confirma que el documento que el denunciante afirma no habérsele facilitado, no formaba parte de su historia clínica, como documento individualizado distinto del posible informe de quirófano.

Por todo lo expuesto, el Director de la Agencia autonómica de la Comunidad de Madrid procede a declarar el archivo del expediente sancionador.

IV.6. El principio de calidad del dato en la actualización del Registro de Vehículos y su implicación en las infracciones de la movilidad

La resolución de 2 de febrero de 2011 se pronuncia sobre la denuncia presentada por un particular contra la Dirección General de Movilidad del Ayuntamiento de Madrid, remitido mediante oficio de la AEPD, por la falta de actualización de los datos de su anterior vehículo, ya que le siguen llegando notificaciones de denuncias de tráfico, cuando la titularidad actual del mismo pertenece a su ex marido como consecuencia de Sentencia de divorcio, habiéndose procedido a dar de baja temporal el vehículo y presentada denuncia ante la Guardia Civil.

Por el Director de la Agencia autonómica se inició procedimiento sancionador contra a dicha Dirección General por infracción del artículo 44.3.f) de la LOPD, que califica como infracción grave: «Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara».

Tramitado el procedimiento de infracción, ha quedado acreditado que la actuación de la Dirección General de Movilidad del Ayuntamiento de Madrid, en relación con los hechos denunciados, se ajusta a lo previsto en la legislación sobre protección de datos, toda vez que el Real Decreto 2822/1998, de 23 de diciembre, por el que se Aprueba el Reglamento General de Vehículos determina en su artículo 2 que la Jefatura Central de Tráfico llevará un Registro de todos los vehículos matriculados, que estará encaminado, preferentemente, a la identificación del titular del vehículo, entre otros cometidos.

Así, tal como se alega por la Dirección General de Movilidad, la normativa expuesta obliga a acudir al Registro de Vehículos de la Jefatura Central de Tráfico para la identificación de la titularidad del vehículo objeto de la actuación policial, con lo que, constatada la titularidad del vehículo, se dirigen al propietario de éste según los datos obrantes en el Registro de Tráfico.

Por su parte, el documento acreditativo de la sociedad de gananciales puede servir para acreditar la identidad del conductor de las infracciones cometidas por el vehículo implicado en este procedimiento, pero no para identificar a su titular, que no pudo modificar su condición en base a estas alegaciones que fueron planteadas ante la Dirección

General de Tráfico, debiendo este identificar al conductor cuando se produce una infracción, de acuerdo al tenor literal del artículo 72.3 del Real Decreto Legislativo 339/1990, de 2 de marzo –vigente en ese momento–.

Finalmente, el Director de la Agencia autonómica madrileña acuerda sobreseer el procedimiento y archivar el expediente sancionador.

IV.7. El principio de calidad del dato en la actualización del Registro de Vehículos y su implicación en las sanciones de tráfico.

En la Resolución de 8 de marzo de 2012, la Agencia autonómica entra a conocer de un caso similar al expuesto en el punto anterior, sobre la actualización de los datos del titular del vehículo en la notificación de los procedimientos por infracción de las normas de circulación y seguridad vial, por parte del Ayuntamiento de Madrid, en relación con el principio de calidad de los datos del artículo 4 de la LOPD.

La Agencia autonómica entra a conocer mediante oficio remitido por la AEPD contra la Dirección General de Movilidad del Consistorio de la capital.

Cabe destacar, que en el curso del procedimiento sancionador son consultados los datos relativos a la titularidad del vehículo y domicilio de los conductores obrantes en los ficheros de la Dirección General de Tráfico, que son actualizados con cada «carga de boletín».

A mayor abundamiento, la Sentencia de la Audiencia Nacional de 27 de febrero de 2008 (sección primera, Roj: SAN 361/2008, ponente: Carlos LESMES SERRANO) se expresa en el siguiente sentido:

«El principio de veracidad o exactitud tiene gran relevancia, en cuanto no sólo resulta necesario que los datos se recojan para su tratamiento de acuerdo con una serie de criterios (principio de proporcionalidad) y que los mismos se empleen para finalidades compatibles a las que motivaron la recogida (principio de finalidad), sino que también exige que quien recoge y trata datos de carácter personal garantice y proteja que la información sometida a tratamiento sea exacta y esté puesta al día.

El incumplimiento o vulneración del principio de veracidad puede tener importantes consecuencias para el afectado, como ocurre en el caso enjuiciado, en el que se han incoado indebidamente al denunciante hasta siete procedimientos sancionadores por infracciones de tráfico por parte del Ayuntamiento de Madrid.

No obstante el recurrente discute que se haya infringido en el presente caso el referido principio ya que a su juicio la actuación realizada fue debida a un error, por la coincidencia de nombre y primer apellido del denunciante con el del conductor habitual del Peugeot Boxer, sin que el dato facilitado al Ayuntamiento fuera por lo demás inexacto, falso u obtenido ilegítimamente. Este razonamiento, en el que se mezcla la falta de culpabilidad con la falta de tipicidad, no puede ser aceptado. Por un lado existió tratamiento de datos inexactos, siendo correcta la calificación de los hechos realizada por la Agencia de Protección de Datos. El hecho imputado consiste precisamente en asociar un nombre y apellidos con un vehículo determinado, con el que se habían cometido determinadas infracciones de tráfico, y tal asociación de datos de carácter personal era claramente inexacta

como el propio recurrente reconoce, ya que la persona a la que corresponden el nombre y apellidos facilitados al Ayuntamiento no era la conductora de tal vehículo, como tampoco era titular del mismo la empresa en la que trabajaba. En definitiva, el envío de esa información inexacta al Ayuntamiento constituye sin duda un tratamiento contrario a al principio de calidad del dato».

Por su parte, la Sala de lo Contencioso de la Audiencia Nacional, en Sentencia de 29.06.2001 (sección primera, Roj: SAN 4241/2001, ponente: Fernando Francisco BENITO MORENO), en materia de protección de datos de carácter personal, ha declarado que «... basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia...».

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido o la profesionalidad exigible al infractor. En este sentido la STS de 05.06.1998 (Sala Tercera, sección séptima, Roj: STS 3692/1998, ponente: Manuel GODED MIRANDA) exige a los profesionales del sector «... un deber de conocer especialmente las normas aplicables».

Sorpresivamente, se da la circunstancia de que desde el mes de abril de 2007 la interesada no figura como propietaria de dicho vehículo y así consta en el Registro de Vehículos de la Dirección General de Tráfico, siendo la infracción de fecha posterior, en concreto de 5 de noviembre de 2010.

Por otro lado, la Dirección General de Movilidad del Ayuntamiento de Madrid, a través de las alegaciones presentadas al Acuerdo de inicio del procedimiento, reconoce el error.

Por todo lo expuesto, el pronunciamiento de la Agencia en este caso es contrario al caso inmediatamente anterior, acordando el Director de la misma la imposición de una sanción por la comisión de una infracción grave tipificada en el artículo 44.3 f) de la LOPD, por vulneración del principio de calidad de los datos previsto en el artículo 4 de la LOPD.

V. Breve conclusión

Aunque *a priori* la observancia del principio de calidad de los datos pueda parecer una cuestión accesoria o de mínima importancia –en comparación con otros procedimientos regulados *in extenso* en la LOPD y en su Reglamento de desarrollo, como el procedimiento sancionador en sus vertientes varias– mediante el presente Trabajo he pretendido demostrar justamente lo contrario, es decir, la importancia de su cumplimiento por parte de las Administraciones Públicas, las empresas y los particulares, así como las consecuencias jurídicas que derivan de su no cumplimiento.

En este sentido, el cumplimiento del mencionado principio garantiza la exactitud y actualización de los datos objeto de consulta, otorgando confiabilidad al sistema del que formen parte, así como evitando la mutación de errores en la cadena de tratamiento lícito de dichos datos por terceras entidades, órganos o personas autorizadas –aun involuntariamente–, lo que podría conllevar nuevas infracciones y efectos indeseados para todas las partes.

De otro lado, el incumplimiento del mismo acarrea la imposición de sanciones –en algunos casos de sustanciosa cuantía– por parte de las Agencias de protección de datos, así como la obligación de la adopción de las medidas correctoras que se consideren pertinentes para la subsanación de las deficiencias puestas de manifiesto, como hemos tenido ocasión de comprobar *supra*.

VI. Bibliografía citada y materiales complementarios

APARICIO SALOM, J., «La calidad de los datos: Título II. Principios de la Protección de Datos, artículo 4», en TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Iª edición, Madrid, Civitas, 2010.

FUENTETAJA PASTOR, J. y MEDINA GONZÁLEZ, S., *La Protección de Datos en la Administración Local*, Iª edición, Iustel, Madrid, 2008.

GICHOT REINA, E., *Datos personales y Administraciones Públicas*, Iª edición, Madrid, Civitas, 2005.

MESTRE DELGADO, J.F., «La protección de datos y los derechos de los interesados en el procedimiento administrativo común», en *VI Curso sobre Régimen de Universidades Públicas*, Almería, Universidad de Almería, 2002.

PIÑAR MAÑAS, J.L., «Protección de datos personales y Entidades Locales», en PARADA VÁZQUEZ, R., y FUENTETAJA, J.A., *Reforma y retos de la Administración Local,* Iª edición, Madrid, Marcial Pons, 2007.

TRONCOSO REIGADA, A., «Principios de la Protección de Datos: el principio de calidad de los datos (Iª parte)», en TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Iª edición, Madrid, Civitas, 2010; *ídem* «Principios de la Protección de Datos: el principio de calidad de los datos (IIª parte)».

VELEIRO REBOREDO, B., *La Protección de Datos de Carácter Personal*, Iª edición, Madrid, Editorial Boletín Oficial del Estado, 2009.

Memorias de la AEPD 1997, 2001, 2002, 2004 (*inspección*).

Página Web de la AEPD en Internet, bases de datos y materiales asociados (disponible en: www.agpd.es; fecha de consulta: 22.12.2013).