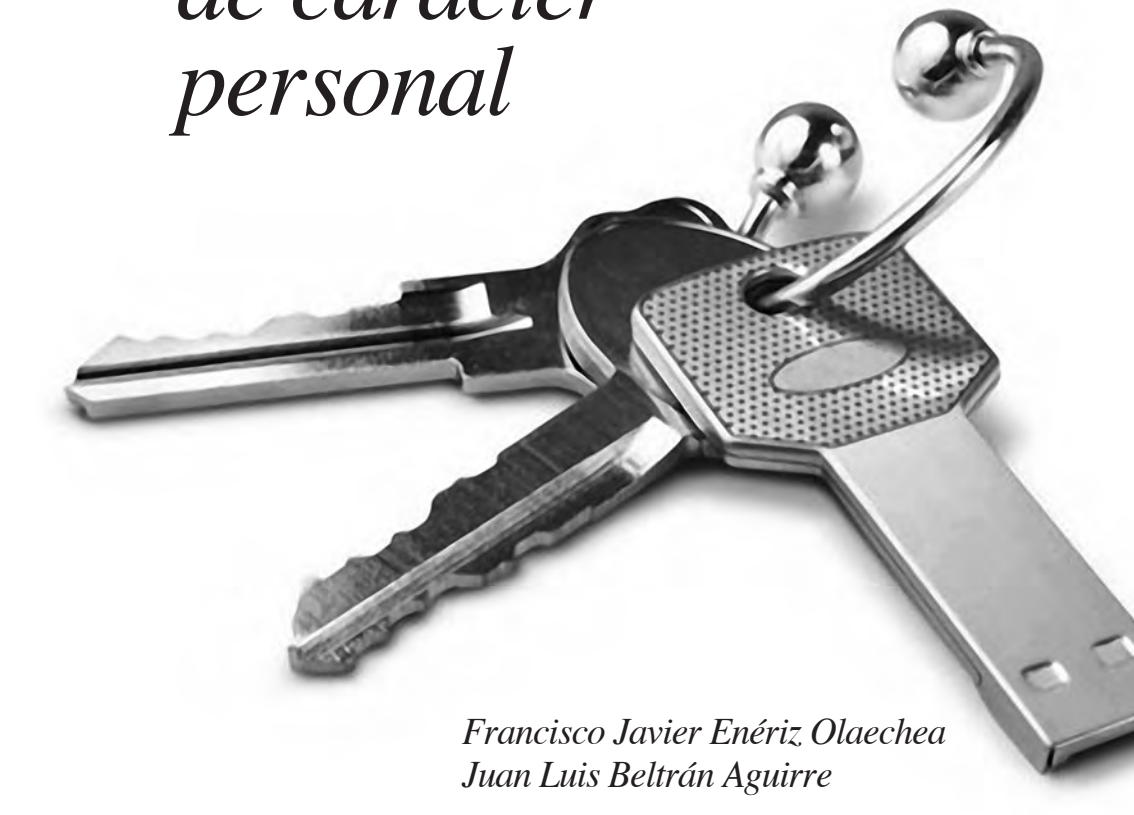
La protección de los datos de carácter personal



Francisco Javier Enériz Olaechea
Juan Luis Beltrán Aguirre

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

Francisco Javier Enériz Olaechea

Juan Luis Beltrán Aguirre

Pamplona 2012

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

Título**: La protección de los datos de carácter personal**

Edita*:* Institución del Defensor del Pueblo de la Comunidad Foral de Navarra

Diseño y maquetación: Carlos Fernández Prego

Imprime:

Depósito Legal: NA 1674-2012

INDICE

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos.
Art., arts.	Artículo, artículos.
BOE	Boletín Oficial del Estado.
CE	Constitución Española.
INSS	Instituto Nacional de la Seguridad Social.
IRPF	Impuesto sobre la Renta de las Personas Físicas.
LBAP	Ley 4/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
LGT	Ley 58/2003, de 17 de diciembre, General Tributaria.
LO	Ley Orgánica.

LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
p.	página.
RPDP	Reglamento de la Ley Orgánica de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.
SNS	Servicio Navarro de Salud.
STC, SSTC	Sentencia(s) del Tribunal Constitucional.
STS, SSTS	Sentencia(s) del Tribunal Supremo.
TC	Tribunal Constitucional.
TS	Tribunal Supremo.
TSI	Tarjeta Sanitaria Indicidual.

PRESENTACIÓN

Dentro de las distintas materias que son objeto de preocupación de los ciudadanos figura, sin duda, la protección de sus datos de carácter personal. Así nos lo revelan las quejas que nos llegan a la oficina del Defensor del Pueblo de Navarra en esta materia y también las distintas noticias que aparecen publicadas en los medios de comunicación.

La protección de los datos de carácter personal es un área de actividad compleja. Lo es porque tan cierto como que toda persona tiene derecho a su intimidad personal, a su propia imagen y a mantener y salvaguardar sus características o elementos de su personalidad sin que nadie pueda invadirlos o desconocerlos de una forma ilegítima, igualmente, existen otros derechos y libertades que actúan en las proximidades de ese derecho y que, en no pocas ocasiones, colisionan con él.

Hoy el Derecho no reconoce derechos subjetivos absolutos, ni clasifica unos por encima de otros a modo de una jerarquía en la que existan derechos de primera, de segunda o de tercera clase. El Derecho moderno parte, como reflejo de la sociedad democrática en la que nace y a la que sirve, de la pluralidad de individuos, entes, actos, derechos, etcétera, y, por tanto, de buscar la

coexistencia pacífica y la colaboración e interrelación entre todos ellos. Este pluralismo social se traduce en que todo derecho subjetivo ha de convivir con los demás, ponderarse con otros y, más que prevalecer en términos absolutos unos sobre otros, ha de ser protegido y, en caso necesario, amparado y restaurado cuando haya podido ser lesionado o desconocido en cada situación concreta. Esta es la filosofía moderna, que renuncia a declarar derechos absolutos o a priorizar de modo categórico unos derechos sobre otros con independencia del caso singular (como bien lo pone de manifiesto la STS de 16 de diciembre de 2010).

Tal concepción moderna se encuentra perfectamente recogida en la teoría que regula la protección de los datos de carácter personal. Tal vez porque su origen no es español en el sentido estricto del territorio de proveniencia, sino europeo o, más precisamente, comunitario. El derecho a la protección de datos de carácter personal aparece reflejado en el artículo 16 del Tratado de Funcionamiento de la Unión Europea y en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea de 2000, y su regulación se encuentra en una Directiva comunitaria, que, prontamente, será sustituida por un Reglamento de la Unión Europea y, por ello, las previsiones de este serán de aplicación directa en el Estado español. En la normativa comunitaria sobre la protección de datos, este derecho se encuentra reconocido, pero su protección es instrumental para el ejercicio de otros derechos y libertades públicas y de ahí que no tenga valor absoluto, ni pueda siquiera prevalecer sobre el derecho al que sirve. Es decir, es un derecho que cede ante otros derechos en los casos concretos, ponderadas las circunstancias y en los términos que la Ley lo exija.

Y la complejidad del derecho a la protección de datos personales también deriva de esa prolija normativa comunitaria y de la

Ley Orgánica en que esta se ha reflejado en el Derecho interno. Si por algo se caracteriza esta normativa es por sentar determinados principios generales que configuran el derecho, para acto seguido incluir un elevado número de supuestos que los excepcionan. El mejor ejemplo de ello puede verse en el principio del consentimiento necesario del afectado tanto en el tratamiento como en la cesión de los datos personales. Este principio general, nuclear de la materia, se ve exceptuado en todos los casos en que así lo prevea, además de la Ley Orgánica de Protección de Datos Personales, una ley sectorial, siendo cada vez más abundantes las leyes que introducen excepciones al respecto.

Este pequeño libro profundiza en este y en otros aspectos referidos al derecho subjetivo a la protección de los datos de carácter personal y a la regulación positiva de la protección de esos datos. Su contenido se estructura en dos grandes partes, con dos enfoques notoriamente diferentes, aunque, obviamente, complementarios.

En la primera parte se aborda con un carácter general la protección de los datos de carácter personal. No se pretende en esta parte realizar un estudio profundo de la materia, ni agotar todos los muchos problemas que su realidad suscita. Por el contrario, si algo se intenta es sentar de una forma muy sencilla las ideas generales que inspiran la protección de los datos personales y el derecho a la misma, para que quien penetre en este campo pueda orientarse y reconocer los puntos cardinales del derecho y los elementos esenciales. De este modo, en esta parte se recuerda la finalidad de la protección, que no es otra que garantizar el derecho de los individuos a que sus datos de carácter personal no sufran intromisiones ilegítimas de terceros. Segui-

damente, se definen los elementos de la protección: el bien jurídico a proteger, que son los demás derechos; el sujeto protegido, que es la persona física titular del derecho; el elemento protegido, que es el dato de carácter personal; en qué actos opera la protección, que es en el doble campo del tratamiento y de la cesión de los datos; y el ámbito material de los ficheros de datos.

Esencial para entender mejor la protección legal de los datos personales es conocer cuáles son los principios aplicables al tratamiento de los datos personales. En esta obra se resumen en siete: fin legítimo, consentimiento del afectado, proporcionalidad, veracidad del dato, licitud del dato, acceso al dato y vida útil del dato. Como se explica en su lugar correspondiente, los dos primeros se perfilan como los más importantes.

En el punto siguiente de esta primera parte se analizan los llamados "datos especialmente protegidos", que son aquellos que merecen un mayor grado de protección legislativa, administrativa y judicial por estar más intensamente relacionados con la personalidad y con la intimidad del individuo.

Otro punto que se destaca es el que el derecho a la protección de datos de carácter personal se configura como un derecho de derechos; es decir, este derecho fundamental se traduce en un conjunto o haz de facultades que su titular puede hacer valer ante terceros. De esta manera, forman parte del derecho a la protección de los datos personales, el derecho a ser previamente informado en la recogida de datos, el derecho a la impugnación de valoraciones que se contengan, el derecho de consulta al registro general de protección de datos, el derecho a obtener una indemnización y los personalísimos e importantes derechos de

acceso, rectificación, cancelación u oposición. A este conjunto de derechos del titular del derecho, se corresponden los deberes de los responsables o encargados de los ficheros, cuales son los de seguridad de los datos y secreto profesional.

La protección que la legislación otorga a las personas no es la misma según los ficheros en los que puedan terminar sus datos personales sean de titularidad pública o de titularidad privada. De ahí que la normativa haga una diferenciación en el régimen de unos y otros ficheros. Por eso, en el lugar correspondiente de este libro se abordan los ficheros de titularidad de la Administración, parando en algunos de ellos, y los ficheros de titularidad particular y las obligaciones que suponen para sus titulares.

Otro punto que se toca en líneas generales y descriptivas es el de Agencia Española de Protección de Datos en su calidad de autoridad pública independiente encargada de garantizar la protección de los datos personales, sin perjuicio de las funciones tutelares de los órganos judiciales. A esta agencia o ente de Derecho público le compete velar por la normativa y amparar a los ciudadanos en el ejercicio de sus derechos. Autoridad que no es la única en un Estado autonómico como el nuestro, en el que algunas Comunidades Autónomas han creado o tienen previsto crear –o están habilitadas al menos- sus respectivas autoridades equivalentes a la Agencia Española de Protección de Datos en cuanto a los ficheros de titularidad pública autonómicos.

Concluye esta primera parte con la parte referida a las infracciones y sanciones que establece la Ley Orgánica de Protección de Datos Personales, aquí sí en términos muy descriptivos.

En la segunda parte se aborda un ámbito muy sensible en la protección de datos personales, ámbito que, posiblemente, sea el que más problemática de tipo práctico y jurídico plantea. Nos referimos al de los datos relativos a la salud, respecto de los que la ciudadanía manifiesta un especial interés en su protección al objeto de que no sean accesibles ni conocidos por terceras personas sin su aprobación o consentimiento. En efecto, los datos de salud se sitúan en la esfera más íntima de la persona, particularmente, aquellos datos que su conocimiento por otras personas puede menoscabar el desarrollo de la personalidad, como lo son los datos relativos a la orientación sexual, al padecimiento de enfermedades psiquiátricas o de transmisión sexual o infecciosas, a embarazos interrumpidos, a la fertilidad, a ser alcohólico o exalcohólico, drogadicto, etc. Su tratamiento inadecuado puede vulnerar otros derechos de la persona afectada, particularmente, el derecho fundamental a la no discriminación. De ahí que la Ley Orgánica de Protección de Datos haya calificado los datos de salud como especialmente protegidos.

Se inicia esta segunda parte con una exposición de la legislación aplicable, dado que en la protección de datos de salud confluyen dos bloques legislativos bien diferentes: de un lado, la propia normativa general de protección de datos personales, y, de otro lado, la legislación sanitaria, tanto la básica estatal como las autonómicas, que tiene la misma, o incluso más relevancia, que la propia legislación de protección de datos personales. Se identifica y analiza, además, la documentación clínica que en los centros y servicios sanitarios contiene datos de salud de las personas.

Seguidamente, se analiza el tratamiento que ha de hacerse de los datos de salud desde su condición de especialmente prote-

gidos. Aquí, además de todas las medidas de seguridad exigibles, se estudia con especial detenimiento lo relativo a la información que ha de facilitarse al interesado, la necesidad de obtener su consentimiento para el tratamiento de sus datos de salud, y las diversas excepciones que la legislación contempla respecto de la necesidad de obtener el consentimiento expreso.

Continúa esta segunda parte desentrañando el contenido y alcance del derecho del paciente al acceso a sus propios datos de salud, estén o no informatizados, la capacidad jurídica para ejercer el acceso, con particular detenimiento en la problemática del menor de edad con 14 años cumplidos, así como las diversas fórmulas para hacer efectivo el derecho de acceso, identificando y analizando también los límites al acceso que prevé la legislación. Termina el capítulo exponiendo el régimen jurídico para la rectificación y la cancelación de los datos de salud por parte de su titular, así como la oposición a su tratamiento.

Termina esta parte haciendo una exposición con vocación de exhaustividad del régimen de acceso a los datos de salud de un sujeto por terceras personas. Se identifican, dedicándose un apartado a cada uno de ellos, los diferentes colectivos de personas a los que se posibilita el acceso y, en su caso, el tratamiento (familiares, profesionales sanitarios, investigadores, inspectores, epidemiólogos, jueces, fiscales, defensores del pueblo, policías, etcétera), y respecto de cada uno de ellos se describe su específico y particular régimen, más o menos limitado, de acceso y de tratamiento de los datos de salud de otras personas.

Para concluir esta presentación, no podemos menos que agradecer al Instituto Navarro de Administración Pública (INAP) y al Departamento de Presidencia del Gobierno de Navarra su

amable colaboración en la preparación de una jornada de cuyo desarrollo nació este pequeño libro, así como las facilidades que nos ha dado para su difusión. Y nuestro agradecimiento también al personal de esas instituciones y del Defensor del Pueblo de Navarra que han posibilitado que, finalmente, el libro viera la luz.

Pamplona, septiembre de 2012

Francisco Javier Enériz Olaechea
Defensor del Pueblo de Navarra
Nafarroako Arartekoa

Juan Luis Beltrán Aguirre
Asesor Jefe del Defensor del Pueblo de Navarra

PARTE I

LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

Francisco Javier Enériz Olaechea
Defensor del Pueblo de Navarra

1. REGULACIÓN: FINALIDAD. EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Como es sabido, los datos de carácter personal se regulan y protegen en España por la Ley Orgánica 15/1999, de 13 de diciembre[1] (LOPD), y, en su desarrollo, por el Reglamento aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Según el artículo 1 de esta Ley Orgánica, su objeto es garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente, los derechos a su honor

1 Derogó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

e intimidad personal y familiar, frente a lo que se llama el "tratamiento" de los datos personales.

Por tanto, esta Ley Orgánica regula, y lo hace de una forma muy detallada, el derecho que tienen las personas físicas a que sus datos de carácter personal no padezcan intromisiones ilegítimas por quienes los conozcan y traten[2].

Este derecho a la protección de datos personales ha ido adquiriendo cada vez mayor relevancia en el ordenamiento jurídico y en la vida social con motivo de las modernas tecnologías de la comunicación, que hacen más fácil su difusión de forma masiva. Y su reconocimiento ha ido ganando terreno en todos los campos: en el sanitario, en el policial, en el informático, en el administrativo, en el comercial, etcétera.

El Tribunal Constitucional ha considerado finalmente el derecho a la protección de los datos de carácter personal como un "derecho fundamental", vinculándolo con el art. 18.4 CE[3], que establece que "la ley limitará el uso de la informática para ga-

2. Pero como declara la sentencia de 20 de mayo de 2003, del Tribunal de Justicia de la Unión Europea, "el principio de no injerencia de la autoridad pública en el ejercicio del derecho a la vida privada, admite (…) que una injerencia de este tipo sea posible en tanto en cuanto esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás".

3. Así aparece citado como tal derecho fundamental a la protección de datos de carácter personal, entre otras, en las sentencias del Tribunal Constitucional 202/1999, de 9 de noviembre, 290/2000, de 30 de noviembre, 292/2000, de 30 de noviembre, 85/2003, de 8 de mayo, 43/2009, de 12 de febrero, y 44/2009, de 12 de febrero; y en los Autos 155/2009, de 18 de mayo, y 20/2011, de 28 de febrero. Interesa destacar la STC 290/2000, de 30 de noviembre, que menciona este derecho con la denominación de "derecho fundamental a protección de datos personales frente a la informática o, si se quiere, a la libertad informática" (F. 7).

rantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos". Por ello, se trata de un derecho protegido por las mayores garantías: así, entre las normativas, por la reserva de ley orgánica; entre las judiciales, además de por el proceso ordinario, por un proceso sumario y preferente; y, sobre ellas, además, por el recurso de amparo ante el Tribunal Constitucional.

La Carta de los Derechos Fundamentales de la Unión Europea, adoptada en 2000, y hoy con un valor jurídico vinculante al menos en todo lo que son políticas comunitarias o con efectos sobre los Estados de la Unión Europea, en su artículo 8, lo ha reconocido y proclamado de una forma expresa y moderna. El precepto afirma que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan[4]". Seguidamente, añade que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley", imponiendo así unos deberes claros a los poderes públicos y a los particulares. Desglosa el derecho, entre otras facultades, en las de "acceder a los datos recogidos que la conciernan y a su rectificación". Y, finalmente, garantiza que "el respeto de estas normas quedará sujeto al control de una autoridad independiente".

En similares términos, el artículo 16 del Tratado de Funcionamiento de la Unión Europea (versión consolidada subsiguiente al Tratado de Lisboa de 2007) reconoce que "toda persona tiene

4. Véase sobre el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, las sentencias del Tribunal de Justicia de la Unión Europea de 9 de noviembre de 2010 y de 24 de noviembre de 2011. Ambas afirman que, con carácter general, este derecho se aplica a toda información sobre una persona física identificada o identificable.

derecho a la protección de los datos de carácter personal que le conciernan". El precepto faculta al Parlamento Europeo y al Consejo para establecer, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. Por último, somete el respeto de estas normas al control de autoridades independientes.

Estas disposiciones generales del Tratado de Funcionamiento de la Unión Europea y de la Carta de Derechos Fundamentales de la Unión Europea se desarrollan y concretan en la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos. Esta es hoy la norma comunitaria de referencia, que la LOPD transpone al Derecho español y que, por su condición de acto legislativo comunitario, ha de respetarse por el Estado español ante la Unión Europea. Por ello, las posibles transgresiones que se produzcan respecto de la Directiva son controladas jurisdiccionalmente por el Tribunal de Justicia de la Unión Europea, cuyas sentencias son vinculantes y obligan a los Estados miembros.

En la actualidad, el Parlamento Europeo y el Consejo están tramitando un proyecto de Reglamento General para la Protección de los Datos Personales, que sustituirá a la Directiva, será la norma de la Unión Europea de referencia para los Estados y

para los ciudadanos en cuanto a la protección de los datos de carácter personal, y, además, dada su cualidad de reglamento comunitario y a diferencia de las directivas, tendrá efecto directo en los Estados miembros y podrá ser alegada inmediatamente por los ciudadanos. El hecho de la sustitución de la Directiva por el Reglamento traerá cambios de trascendencia en la regulación de la protección de los datos de carácter personal, lo cual puede significar que no solo haya que modificar la LOPD en algún punto concreto para que la norma estatal cohoneste, como es su obligación, con la nueva norma comunitaria, sino incluso que haya que redactar una nueva Ley Orgánica adaptada plenamente a dicho Reglamento de la Unión.

El proyecto de Reglamento General de Protección de Datos se caracteriza por la continuidad de las líneas esenciales que estableció la Directiva 95/46/CE. Los objetivos y principios de esta Directiva continúan estando recogidos en el Reglamento. Pero, al mismo tiempo, como es lógico, el Reglamento buscar perfeccionar el sistema de protección de los datos personales en toda la Unión, aclarando las dudas que ofrecía la normativa anterior, mejorando sus previsiones y preocupándose por dar un tratamiento completo y uniforme en todos los Estados miembros. Su objeto y principios generales son básicamente los mismos; ahí hay poco cambio. Donde están las novedades está en el refuerzo de los derechos del interesado, fundamentalmente en lo relacionado con la transparencia, la información y el acceso a los datos, potencia el derecho al olvido y a la supresión de los datos. También relaciona mejor las obligaciones de los responsables del tratamiento y de los encargados de estos. Refuerza las garantías para la seguridad de los datos, destacando la imposición del deber del responsable del tratamiento de no-

tificar a la autoridad de control en un plazo de veinticuatro horas cualquier violación de datos personales. Introduce la obligación para el responsable o el encargado de efectuar una evaluación del impacto de las operaciones de tratamiento cuando las operaciones entrañen riesgos para los derechos y libertades de los interesados. Introduce, como una garantía más, la figura del delegado de protección datos, obligatoria en organismos públicos y empresas de mayor tamaño, con funciones de vigilancia en todas las cuestiones relativas a la protección de datos. Apuesta por los códigos de certificación con el fin de contribuir a una mejor aplicación y a la calidad en la gestión del os datos personales. Refuerza la independencia y las funciones de las autoridades públicas de control, encargadas de supervisar la aplicación de la normativa europea, al tiempo que impulsa la cooperación y coherencia de las autoridades de control. Crea el Consejo Europeo de Protección de Datos como órgano independiente encargado de velar por la aplicación coherente del Reglamento en toda la Unión. Establece un completo régimen de reclamaciones ante las autoridades de control, de recursos judiciales tanto contra las decisiones de las autoridades de control como contra los responsables y encargados del tratamiento, fija responsabilidades y el derecho a la indemnización, e impone la obligación a los Estados de establecer sanciones administrativas por vulneraciones a la normativa, cuya imposición compete a las autoridades de control. Cierra sus previsiones con disposiciones específicas para garantizar la compatibilidad entre el tratamiento de datos personales y la libertad de expresión, la salud, los derechos de los trabajadores en el ámbito laboral, los fines de investigación histórica, estadística o científica, las iglesias y asociaciones religiosas y la obligación de secreto profesional.

También algunos Estatutos de Autonomía recientemente reformados, como el de Cataluña en su redacción de 2006, el de Andalucía, en su redacción de 2007, el de Aragón, también de 2007, o el de Castilla y León, igualmente de 2007, lo recogen como un derecho. El artículo 31 del Estatuto de Autonomía de Cataluña señala que "todas las personas tienen derecho a la protección de los datos personales contenidos en los ficheros que son competencia de la Generalitat y el derecho a acceder a los mismos, a su examen y a obtener su corrección. Una autoridad independiente, designada por el Parlamento, debe velar por el respeto de estos derechos en los términos que establecen las leyes". Por su parte, el artículo 32 del Estatuto de Autonomía de Andalucía, con un ámbito más limitado que el catalán, afirma que "se garantiza el derecho de todas las personas al acceso, corrección y cancelación de sus datos personales en poder de las Administraciones públicas andaluzas". El artículo 16.3 del Estatuto de Autonomía de Aragón dispone que "todas las personas tienen derecho a la protección de sus datos personales contenidos en las bases de datos de las Administraciones Públicas y empresas públicas aragonesas y las empresas privadas que trabajen o colaboren con ellas. Igualmente, tendrán derecho a acceder a los mismos, a su examen y a obtener su corrección y cancelación".

El artículo 12 d) del Estatuto de Castilla y León incluye este derecho como una manifestación del derecho a la buena administración, y dispone que "la ley garantizará los siguientes derechos de los ciudadanos en sus relaciones con la Administración autonómica: (…) a) A la protección de los datos personales contenidos en los ficheros dependientes de la Administración autonómica, garantizándose el acceso a dichos datos, a su exa-

men y a obtener, en su caso, la corrección y cancelación de los mismos. Mediante ley de las Cortes podrá crearse la Agencia de Protección de Datos de la Comunidad de Castilla y León para velar por el respeto de estos derechos en el marco de la legislación estatal aplicable".

Lo cierto es que el derecho aparece en el ordenamiento jurídico español perfecta y completamente regulado en todos sus elementos en la citada LOPD, por lo que esta se convierte en el marco principal y general de este derecho fundamental.

Desde la perspectiva de su naturaleza jurídica, nos encontramos ante un derecho fundamental, dotado de identidad propia y diferenciada respecto a otros derechos, pero al servicio de la protección de los demás derechos fundamentales.

Su carácter de "derecho fundamental" hace que se beneficie de las garantías que le otorga la Constitución. La primera, la de su efecto directo e inmediato, ya que, por mor del artículo 51 de la Constitución, vincula a todos los poderes públicos directamente sin necesidad incluso de que una ley lo reconozca o lo regule. La segunda es la garantía de la reserva de ley orgánica, que consiste en que su regulación general ha de efectuarse obligadamente por "ley orgánica" (por ello, la LOPD es una ley orgánica), como lo precisa el artículo 81 de la Constitución, lo que no excluye que determinados aspectos secundarios sean tocados por decretos-leyes o por leyes ordinarias, ni tampoco excluye que la ley orgánica que la regule remita al reglamento la fijación complementaria de determinados aspectos en que así pueda resultar necesario por un excesivo detalle o por razones técnicas. La tercera garantía es

judicial, que significa que la tutela judicial de este derecho no se limita solo a los procesos ordinarios que tienen los derechos ordinarios, sino que también puede el ciudadano titular del derecho fundamental acudir, para obtener el amparo de los órganos judiciales, a un proceso especial basado en los principios de sumariedad y preferencia, como dispone el art. 53.2 de la Constitución (así, por ejemplo, los arts. 114 a 122 de la Ley de la Jurisdicción Contencioso-Administrativa, frente a las resoluciones administrativas). Finalmente, está la garantía del Tribunal Constitucional, que permite al máximo garante de la Constitución declarar inconstitucionales leyes o preceptos que afecten negativamente el derecho[5] o estimar recursos de amparo actos administrativos o judiciales que ignoren o vulneren este derecho fundamental.

Es, además, un derecho autónomo. Tiene entidad diferencia respecto de otros derechos, particularmente del derecho a la intimidad del art. 18.1 CE, tanto en su función, objeto y contenido, aunque comparta con este último el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar (STC 292/2000, de 30 de noviembre). Incluso el objeto de este derecho es más amplio que el objeto del derecho a la intimidad, "ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones el TC ha definido en términos amplios como esfera de los bienes de la personalidad que pertenecen al

5. Como así hizo la STC 292/2000, de 30 de noviembre, con determinados incisos de los arts. 21.1 (sobre comunicación de datos entre Administraciones públicas en ficheros de titularidad pública) y 24 (sobre excepciones genéricas a los derechos de las personas físicas en la recogida de datos) de la LOPD.

ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal, como el derecho del honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del art. 18.4 CE, al pleno ejercicio de los derechos de la persona" (STC 292/2000, de 30 de noviembre). Para el Tribunal Constitucional, el art. 18.4 CE "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que además consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona (…) pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos" (STC 11/1998, de 13 de enero)[6].

Finalmente, es un derecho al servicio de otros derechos fundamentales, ordenado a la protección de otros derechos fundamentales (STC 11/1998, de 13 de enero). El Tribunal Constitucional ha declarado que este derecho "contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos" (por todas, STC 290/2000, de 30 de noviembre). Por ello, dada su función instrumental de otros derechos, estamos ante un derecho subjetivo que juega tanto en el campo de las relaciones jurídico-públicas, como en el de las relaciones jurídico-privadas, por lo que su titular está legitimado para hacerlo valer tanto ante organismos y autoridades públicos, como ante particulares.

6. En el mismo sentido, las SSTC 33/1998, 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 125/1998, 126/1998, 158/1998, 198/1998, 223/1998, 30/1999, de 8 de marzo, 44/1999, de 22 de marzo, y 45/1999, de 22 de marzo.

2. LOS ELEMENTOS DE LA PROTECCIÓN.

A. El bien jurídico protegido.

El bien jurídico que protege el derecho a la protección de datos personales lo son "los derechos fundamentales", todos ellos, sin excepción; pero, en particular, la protección constitucional se dirige al derecho a la intimidad, en su vertiente tanto personal como en su vertiente familiar, al derecho al honor y al derecho a la propia imagen.

B. El sujeto protegido o titular del derecho.

A quien protege este derecho es a las personas físicas titulares de los datos, es decir, a los individuos… mientras estén vivos.

El derecho se aplica igualmente a las personas físicas identificadas o identificables (sentencias del Tribunal de Justicia de la Unión Europea de 9 de noviembre de 2010 y de 24 de noviembre de 2011).

Por ello, quedan excluidos del ámbito subjetivo de aplicación de la LOPD los datos de:

a) Las *personas jurídicas* (sociedades, empresas, Administraciones públicas, etcétera).

b) Los *empresarios individuales*, incluso cuando se haga referencia a ellos en su condición de comerciantes, industriales o navieros.

c) Los *fallecidos*. No obstante, la Ley permite que las personas vinculadas al fallecido por razones familiares o análogas puedan dirigirse a los responsables de los ficheros o tratamientos con la finalidad de notificarles el óbito y solicitarles la cancelación de los datos personales del fallecido.

C. El elemento protegido: el dato de carácter personal.

El elemento u objeto merecedor de la protección jurídica es el "dato de carácter personal".

El concepto legal de dato de carácter personal abarca cualquier información que se refiera a una persona física identificada o –y esto es muy importante– identificable [art. 3 a)], cualquiera que sea el tipo de soporte físico en que aparezca el dato. Se incluyen en este concepto aspectos tales como el nombre y apellidos, la voz, la imagen[7], el sexo, la edad, afiliación, estado civil, el adn, el domicilio, los estudios, el currículum profesional, las actividades profesionales[8], los ingresos profesionales[9], las condiciones de trabajo[10], los datos fiscales, sus propiedades y bienes pa-

7. STS de 16 de diciembre de 2010 (en particular, una fotografía).

8. Las sentencias del TEDH de 16 de febrero de 2000 y 4 de mayo de 2000, consideran que el concepto de "vida privada" que se utiliza en esta materia no excluye las actividades profesionales.

9. Según la sentencia de 20 de mayo de 2003, del TJUE, los datos nominales sobre los ingresos profesionales de un individuo son datos personales.

10. La sentencia de 6 de noviembre de 2003 del TJUE considera que hacer referencia en una página web a personas e identificarlas por su nombre o por otros medios, como un número de teléfono o información relativa a sus condiciones de trabajo, y a sus aficiones, constituye un tratamiento total o parcialmente automatizado de datos personales.

trimoniales[11], los datos relativos a la salud[12], los datos físicos, los datos genéticos[13], los datos biométricos[14], los datos relativos a la salud, la ideología, las creencias, las conductas o hábitos, las aficiones[15], los actos que realice, y un largo etcétera.

La STS de 1 de julio de 2011 efectúa una delimitación positiva y una delimitación negativa de los datos personales. Conforme a su tenor, la delimitación positiva concreta los datos en "informaciones relativas a las personas físicas, es decir, a los hechos, circunstancias o antecedentes del titular de los datos, relativos a cualquier esfera de actuación. En este sentido debemos precisar que esta información puede referirse no solo a la vida privada sino a cualquier otro ámbito en donde la persona física despliegue su actividad, y obviamente extenderse a datos sobre su vida profesional". Conforme a la delimitación negativa, "no pueden comprenderse en el concepto de datos de carácter personal los argumentos, razonamientos, consideraciones, refle-

11. La sentencia de 16 de diciembre de 2008, del TJUE, considera que queda sometido a la Directiva de protección de datos personales, el tratamiento de datos relativos a los rendimientos del trabajo y del capital y al patrimonio de las personas físicas.

12. Por tales datos, entiende el art. 4 del proyecto de Reglamento General de Protección de Datos, "cualquier información que se refiera a la salud física o mental de una persona, o a la asistencia prestada por los servicios de salud a la persona".

13. Por tales datos, entiende el art. 4 del proyecto de Reglamento General de Protección de Datos, "todos los datos, con independencia de su tipo, relativos a las características de una persona que sean hereditarias o adquiridas durante el desarrollo prenatal temprano".

14. Por tales datos, entiende el art. 4 del proyecto de Reglamento General de Protección de Datos, "cualesquiera datos relativos a las características físicas, fisiológicas o conducturales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos".

15. Sentencia de 6 de noviembre de 2003 del TJUE.

xiones, y, en definitiva, las razones sobre las que se sustenta una decisión administrativa". De este modo, las frases empleadas en dicha resolución no son más que el soporte lógico argumental de cualquier resolución motivada que conduce a una conclusión, y que, por tanto, solo pueden ser corregida cuando se cuestiona o se impugna por los medios legalmente previstos al respecto".

Obviamente, la protección se extiende a datos necesariamente "personales", es decir, de personas o de sus características por ser personas; y no se proyecta, por el contrario, sobre datos que no sean personales (como, por ejemplo, las características técnicas de un aparato, etcétera) o que, aún siéndolos, no permitan la identificación de una persona.

Basta, por tanto, que el dato permita identificar a una persona, para que estemos hablando de datos de carácter personal y entre en juego la protección que ofrece el ordenamiento jurídico.

En el ámbito de la protección de los datos personales, juega una función muy válida la llamada "disociación", que es la referencia a hechos o personas tras haber eliminado los datos que permiten su identificación razonable por un tercero. El artículo 11.6 de la LOPD la reconoce expresamente: "si la comunicación de datos de carácter personal se efectúa previo procedimiento de disociación, no se precisa el consentimiento. En todo caso, la disociación ha de ser previa. La disociación es muy útil en la publicación de motivos, exposición de documentos, estadísticas, etcétera. Puesto que , eliminados los datos personales que posibiliten identificar a la persona de referencia no cabe lesión del derecho a la protección de tales datos de carácter personal.

D. Frente al tratamiento o la cesión de los datos.

La protección que otorga el ordenamiento jurídico al dato personal (realmente, a su titular) lo es frente a dos grandes tipos de operaciones:

- El *tratamiento* de los datos, es decir, frente a cualquier clase de acto, operación o procedimiento técnico, tenga carácter automatizado o no, que permita la recogida, grabación, captación, conservación, almacenamiento, elaboración, modificación, bloqueo o cancelación de esos datos[16]; es importante subrayar que ya no se requiere que el tratamiento sea necesariamente automatizado [art. 3c) LOPD].

  La Directiva 95/46 /CE es aún más minuciosa en la enumeración de las operaciones o procedimientos que cons-

16. El Tribunal de Justicia de la Unión Europea considera que hacer referencia en una página web a personas e identificarlas por su nombre o por otros medios, como un número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento total o parcialmente automatizado de datos personales (sentencia de 6 de noviembre de 2003).

    Asímismo, el Tribunal de Justicia de la Unión Europea considera un ejemplo de tratamiento de datos personales los hechos de recoger una sociedad privada de los documentos públicos de la administración fiscal, datos relativos a los rendimientos del trabajo y del capital y al patrimonio de las personas físicas y tratarlas para su aplicación, publicarlos por orden alfabético y por tipos de rentas en listas pormenorizadas clasificadas por municipios, cederlos en diversos CD-ROM para que sean utilizados con fines comerciales, y tratarlos en un servicio de mensaje de texto (SMS), que permite a los usuarios de teléfonos móviles, enviando el nombre y el municipio en el que reside una persona física, recibir información relativa a los rendimientos del trabajo y del capital, así como del patrimonio de esa persona. Considera que estos hechos están sometidos a la Directiva de protección de datos personales (sentencia de 16 de diciembre de 2008).

    Véase también sobre el concepto de tratamiento, la STS de 10 de noviembre de 2011.

tituyen tratamiento: recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como bloqueo, supresión o destrucción (STS de 16 de diciembre de 2010). Y más aún lo es el art. 4 del proyecto de Reglamento General de Protección de Datos, que considera tratamiento "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, efectuadas o no mediante procedimientos automatizados, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, supresión o destrucción".

- La *cesión o comunicación* de datos que resulte de comunicaciones, consultas, interconexiones y transferencias, a cualquier persona del sector privado o del sector público, así como frente a los posteriores usos que haga esta de los datos [arts. 3 y 2.1].

La cesión o comunicación se produce cuando se revela un dato a una persona distinta del interesado. Esto incluye las reproducciones y emisiones en tiempo real.

Por tanto, "tratamiento" y "cesión" son, jurídicamente, a efectos de la LOPD, dos tipos de operaciones distintas, y ante cualquiera de las dos (y lo que supongan) están protegidos legalmente los datos personales.

La dificultad para establecer una frontera nítida entre el tratamiento y la cesión ha provocado que el Tribunal Supremo haya sostenido que la cesión de datos no es sino una modalidad del tratamiento (SSTS de 4 de mayo de 2009 y 17 de septiembre de 2010), y, lo que es más importante aún, que el futuro Reglamento General de Protección de Datos solo contemple la figura del "tratamiento", dentro del cual se incluyen la comunicación por transmisión, la difusión, la consulta o el acceso (art. 4), excluyendo ya la cesión como concepto autónomo.

Interesa destacar, en este punto, que la aparición de datos de carácter personal de personas físicas en internet constituye un supuesto de tratamiento y, en todo caso, de cesión de datos, que queda sometido sin excepción al ámbito de aplicación de la LOPD, a los principios de esta Ley y a las garantías y derechos que esta misma norma pone al servicio del ciudadano cuyos datos figuren en la red. Por ello, las personas físicas concernidas pueden ejercer sus derechos de rectificación, oposición y cancelación (estos dos últimos conocidos como "derecho al olvido" en internet), tanto frente al autor de la información, como frente a quien la difunde (el llamado "buscador"), por ser este último, jurídicamente, un prestador de servicios de la sociedad de la información conforme a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información.

E. El ámbito material: los ficheros.

La Ley protege especialmente contra la existencia de los denominados "ficheros" de datos.

Por tal fichero se entiende "todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso". También se les conoce en algún texto legal como "base de datos". Es esencial que el fichero sea un conjunto organizado de datos (SSTS de 19 de septiembre, 7 de noviembre y 19 de diciembre, que no consideran ficheros los Libros de Bautismo; y STS de 10 de noviembre de 2011, que sí considera ficheros la base de datos de una asociación religiosa).

La Ley hace "responsable del fichero o tratamiento" a la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. No es responsable solo quien crea el fichero o quién lo administre, sino quien "decide" sobre él.

Es más, la LOPD distingue entre el "responsable del fichero", que es su titular, y el "encargado del tratamiento". Este último es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trata datos personales por cuenta del responsable del tratamiento.

El TS, consciente de la realidad de la gestión de los datos personales, ha recordado que la LOPD "parte de que, prestado el consentimiento para el tratamiento, el acceso al dato cabe entenderse autorizado igualmente para aquellos empleados que en el cumplimiento de sus funciones tuvieren necesidad de consultar dicho dato personal, y, a tal efecto, el articulo 9.1 de dicha Ley Orgánica impone al responsable y al encargado del tratamiento la obligación de adoptar las medidas de índole técnica y

organizativas necesarias que garanticen la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural, disponiendo el articulo 10 que el responsable del fichero y quiénes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlo, obligaciones que subsistirán aún después de finalizar sus relaciones particulares del fichero o, en su caso, con el responsable del mismo" (STS de 2 de diciembre de 2009), pronunciamiento que atañe incluso a datos especialmente sensibles.

El proyecto de Reglamento General de Protección de Datos añade un agente más a relación jurídica: el delegado de protección de datos. Se trata de una persona física designada por el responsable del tratamiento o por el encargado de esta para asegurar que el tratamiento de los datos personales responde a la normativa comunitaria. Será obligatoria su designación en los tratamientos de los organismos públicos, en empresas de más de 250 personas o en operaciones que requieran un seguimiento periódico y sistemático de los interesados. El delegado debe actuar con independencia y sin estar sujeto a instrucciones en el ejercicio de sus funciones.

Ahora bien, la LOPD no es aplicable a determinados ficheros que ella misma excluye:

- Los ficheros mantenidos por personas físicas *en el ejercicio de actividades exclusivamente personales o domésticas*. Se

consideran como tales actividades las que se inscriben en el marco de la vida privada o familiar de los particulares. Pero, por el contrario, no se pueden considerar tales la difusión de datos personales por internet de modo que resulten accesibles a un grupo indeterminado de personas (sentencia de 6 de noviembre de 2003, del Tribunal de Justicia de la Unión Europea).

- Los ficheros de *personas jurídicas que se limitan a incorporar datos de personas físicas que les prestan sus servicios*, cuando únicamente recojan su nombre y apellidos, las funciones o puestos desempeñados, la dirección postal o electrónica, el teléfono o el número de fax profesionales. Son meras relaciones profesionales, que se dan sobre todo en el ámbito de los colegios profesionales o de las empresas.

- Los ficheros sometidos a la normativa sobre protección de *materias clasificadas*. Son materias reservadas por las leyes por razón de su secreto.

- Los ficheros establecidos para *la investigación del terrorismo y de formas graves de delincuencia organizada*. Solo pueden ser titulares de estos ficheros las autoridades públicas policiales. No obstante, el responsable del fichero debe comunicar previamente a la AEPD la existencia del fichero, su finalidad y sus sus características generales.

El art. 2.2 del proyecto de Reglamento General de Protección de Datos prevé dejar fuera de su ámbito de aplicación material el tratamiento de datos personales "por parte de las

autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales".

Aclara la sentencia de 16 de diciembre de 2008, del Tribunal de Justicia de la Unión Europea que la diferencia de tratamiento, en aras de combatir la delincuencia, entre nacionales y ciudadanos de la Unión que no sean nacionales de un Estado miembro, contituye una discriminación prohibida.

Además de las anteriores, estaría también al margen de la LOPD, aunque se aplicaría esta en los casos de una llamada o remisión expresa a la misma, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Esta Ley obliga a los operadores a conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, y regula el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Se aplica a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. En cambio, se excluye de su ámbito de aplicación el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas. Los destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley son los operadores que presten

servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Por otro lado, existen ficheros que se rigen por una normativa especial, pero a los que se aplica también la LOPD. Son los siguientes:

a) Los ficheros regulados por la *legislación de régimen electoral*.

b) Los ficheros que *sirven a fines exclusivamente estadísticos* y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los ficheros que tienen por objeto el almacenamiento de los datos contenidos en los *informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas*.

d) Los ficheros derivados del *Registro Civil y del Registro Central de penados y rebeldes*.

e) Los ficheros procedentes de imágenes y sonidos obtenidos mediante la utilización de *videocámaras por las Fuerzas y Cuerpos de Seguridad*, de conformidad con la legislación vigente. Aquí es obligado recordar que la Ley Orgánica 4/1997, de 4 de agosto, autoriza a las Fuerzas y Cuerpos de Seguridad la utilización de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos

o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como para prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La LOPD sí que es plenamente aplicable a los tratamientos de imágenes de personas físicas con fines de vigilancia, obtenidas con sistemas de cámaras y videocámaras, cuando dicha vigilancia ya no se hace por las Fuerzas y Cuerpos de Seguridad, sino por otros sistemas públicos o privados. Este tratamiento se somete a lo dispuesto en la Instrucción 1/2006, de 8 de noviembre, de la AEPD. Esta instrucción dispone que:

- Los responsables de los sistemas de videovigilancia deben colocar, en las zonas videovigiladas un distintivo informativo, ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados, y tener a disposición de los interesados impresos en los que se detalle la información que requiere la LOPD.

- Las cámaras instaladas en espacios privados no pueden obtener imágenes de espacios públicos, salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En la práctica, por tanto, sí que pueden obtenerse esas imágenes de los espacios públicos.

- En todo caso, debe evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida. La finalidad es la

protección del edificio frente a posibles ataques a las personas, la propiedad privada, la integridad de los elementos físicos, etcétera.

- Los datos han de cancelarse en el plazo máximo de un mes desde su captación.

- La creación de esos ficheros de videovigilancia, cada vez más abundantes, debe notificarse previamente a la AEPD, para su inscripción en el Registro General de Protección de Datos. Si el fichero es público, ha de crearse mediante una disposición general. Lo aquí dispuesto no se aplica si el tratamiento consiste exclusivamente en la reproducción o emisiones de imágenes en tiempo real.

3. PRINCIPIOS GENERALES APLICABLES AL TRATAMIENTO DE LOS DATOS PERSONALES.

Para que el tratamiento de datos (en concreto, la recogida de datos y cualquier operación posterior con ellos) sea acorde con la Ley, ha de cumplir una serie de principios generales[17].

Esto, como ya se ha visto, se afirma muy sintetizadamente en el art. 8.2 de la Carta de Derechos Fundamentales de la Unión Euro-

17. Estos principios generales que legitiman el tratamiento de los datos relativos se recogen en los artículos 6 y 7 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

    Véanse, al respecto de estos principios, las sentencias del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2003, 6 de noviembre de 2003, 16 de noviembre de 2008 y 24 de noviembte de 2011. Esta última sentencia aclaró que, sobre estos principios, los Estados miembros no pueden añadir otros nuevos, ni imponer exigencias adicionales que vengan a modificarlos.

pea. En este artículo, tras reconocerse que toda persona tiene derecho a la protección de datos de carácter personal que le conciernan, se afirma que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley".

Tales principios generales, pero en cualquier caso auténticas normas exigibles, son:

A. El principio de calidad de los datos: fin legítimo y proporcionalidad.

Bajo este nombre del principio "de calidad de los datos[18]", se encuentran realmente otros dos principios generales:

El primero es el *principio del fin o interés legítimo*. Significa que el tratamiento de los datos ha de responder a una finalidad determinada, explícita y legítima, y que cualquier operación que se haga debe ajustarse al fin para el que se hayan obtenido los datos[19]. Este principio es, junto con el del consentimiento del afectado, uno de los más importantes y el que, desde un punto de vista práctico, da más sentido a todo el conjunto del ordenamiento sobre la protección de los datos de carácter personal.

El principio de fin o interés legítimo exige que, en el caso de que no exista consentimiento del interesado, se respeten los de-

18. Sobre el principio de calidad, las sentencias de 20 de mayo de 2003, 16 de diciembre de 2008 y 24 de noviembre de 2011, del Tribunal de Justicia de la Unión Europea.

19. Sobre el principio del interés legítimo o fin legítimo, véase la sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, y la interpretación que da al artículo 7, letra f). de la Directiva 95/46.

rechos y libertades fundamentales de éste y que dichos datos figuren en fuentes accesibles al público, excluyendo de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes (sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011).

El principio supone que los datos de carácter personal que sean objeto de tratamiento no pueden usarse para finalidades incompatibles o diferentes con aquellas para las que los datos hubieran sido recogidos. Aclara la Ley que no se considera incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

El segundo de los principios que integran la calidad de los datos es el principio de *proporcionalidad*, también llamado de pertinencia (STS de 12 de marzo de 2012) Conforme a este, la recogida y el tratamiento de los datos han de ser adecuados, pertinentes y no excesivos. O dicho de otro modo, no se puede recoger más datos que los estrictamente necesarios, con la finalidad que se pretende y en la materia de que se trate[20]. Una recogida abusiva de datos es, desde luego, contraria a este principio y supone la ilegalidad del tratamiento.

B. El principio del consentimiento del afectado. Excepciones.

Es, desde luego, el principio esencial de la protección de datos personales, al mismo plano, al menos, que el citado principio del fin legítimo.

20. Véase la sentencia del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2003.

Como afirma el art. 8.2 de la Carta de Derechos Fundamentales de la Unión Europea, el tratamiento de los datos de carácter personal requiere el consentimiento previo del afectado. Por consentimiento se entiende "la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado autoriza o permite el tratamiento de datos personales que le conciernen". No quiere decirse que la manifestación sea siempre expresa, sino libre e inequívoca (SSTS de 20 de mayo y 12 de noviembre de 2011 y de 23 de enero de 2012), por lo que también vale, para los datos no especialmente protegidos, que la expresión de voluntad sea tácita o que el consentimiento no lo sea explícito. Así ocurre cuando el responsable del fichero concede un plazo para que el interesado manifieste su oposición a la incorporación del dato al fichero y en ese plazo el interesado no se posiciona o no dice nada en contra.

La STS de 23 de enero de 2012 recuerda que el consentimiento para el tratamiento de datos que exige el art. 6.1 de la LOPD ha de ser inequívoco y previo: a) "inequívoco es lo que no admite duda o equivocación, y por contraposición a equívoco, lo que no puede entenderse en varios sentidos, de forma que aunque no sea exigible un consentimiento en forma escrita, al no exigirlo para el supuesto del que tratamos ningún precepto legal, la entidad que pretenda obtener este consentimiento inequívoco deberá arbitrar los medios necesarios para que no queden dudas de la que cesión de los datos ha sido consentida"; b) "el consentimiento ha de ser previo, requisito que tampoco reúnen los consentimientos de los trabajadores en los que declaran que consienten expresamente que se trataran sus datos para prestarles la asistencia sanitaria necesaria, todos ellos fechados y firmados con posterioridad al año 2004, por

lo que no pueden amparar las cesiones anteriores de datos de trabajadores".

Como principio general que es, el principio del consentimiento del afectado, que ha de ser en todo caso, además de inequívoco, previo (STS de 23 de enero de 2012), tiene excepciones importantes:

a) La primera es que una ley o una norma de Derecho comunitario hace innecesario el consentimiento cuando así lo disponga o exija el tratamiento o la comunicación del dato sin ese consentimiento. Así ocurre cuando una ley sectorial no requiere de forma clara el consentimiento por razones de interés público. Son numerosos los casos en que las Leyes no requieren el consentimiento: a favor de la Hacienda en la LGT, en la Ley del Defensor del Pueblo para el tratamiento de los datos que las quejas contienen o para la cesión de datos de las Administraciones a favor del Defensor, en el caso de transacciones bancarias por blanqueo, y un largo etcétera.

b) Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias. Este es un supuesto que parece que las Administraciones desconocen en la práctica y al que les cuesta acogerse, ya que no se hace necesario el consentimiento de los interesados si una Administración trata o recoge datos para sus competencias públicas en ejercicio de su servicio al interés público.

c) Cuando los datos se refieren a las partes de un contrato o precontrato de una relación negocial, laboral o adminis-

trativa, y son necesarios para su mantenimiento o cumplimiento (art. 6.2 LOPD y STS de 3 de junio de 2009). Es el caso de los ficheros de personal de empresas, por ejemplo.

d) Cuando el tratamiento de los datos tiene por finalidad proteger un interés vital del interesado. Juega, sobre todo, en el campo de la sanidad y de determinados servicios. La LOPD exime el consentimiento del interesado cuando el tratamiento de datos resulta necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que el tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto. Hace falta, por tanto, un fin sanitario y un profesional sanitario o equivalente.

e) Cuando los datos figuran en fuentes accesibles al público y su tratamiento es necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

   Se entiende por "fuentes accesibles al público" aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen la consideración legal de fuentes de acceso público: a) los diarios y boletines oficiales; b) los medios

de comunicación social; c) los censos promocionales; d) las guías de servicios de comunicaciones electrónicas; e) los repertorios telefónicos en los términos previstos por su normativa específica; o f) las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo (datos del domicilio postal completo, número de teléfono, número de fax, dirección electrónica, números de colegiado, fecha de incorporación y situación del ejercicio profesional).

Resulta obligada la lectura de la sentencia de 24 de noviembre de 2011, del Tribunal de Justicia de la Unión Europea, sobre esta excepción. Esta declara que debe interpretarse que se opone a la Directiva 95/46/CE la normativa nacional que, para permitir el tratamiento de datos personales, "exige, en el caso de que no exista el consentimiento del interesado, no solo que se respeten los derechos y libertades fundamentales de este sino, además, que dichos datos figuren en fuentes accesibles al público, excluyendo así, de forma categórica y generalizada, todo tratamiento de datos que no figuren en tales fuentes". Con apoyo en dicha resolución comunitaria, la sentencia de 8 de febrero de 2012, del Tribunal Supremo, anula el artículo 10.2 b) del Reglamento de LOPD, que no requiere consentimiento del interesado en los supuestos de tratamiento o cesión de datos cuando "los datos objeto de tratamiento o cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su trata-

miento o conocimiento, siempre que no se vulneren los derecho y libertades fundamentales del interesado", texto que se corresponde con el de la LOPD.

La comunicación o cesión de datos.

Ya se ha dicho que una cosa es el tratamiento, y otra distinta es la comunicación o la cesión de los datos. En este segundo tipo de operaciones, el principio general a seguir es que los datos de carácter personal solo pueden comunicarse a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado (art. 11.1 LOPD, STC 292/2000, de 30 de noviembre, y SSTS de 14 de octubre de 2009 y 6 de mayo y 20 de mayo de 2011). Como puede verse, nuevamente surgen y son exigibles para la comunicación de datos los principios generales de finalidad legítima y consentimiento, ahora previo en todo caso, e igualmente inequívoco, del afectado.

Ahora bien, la LOPD permite también que los datos de carácter personal puedan cederse sin contar con el consentimiento del interesado cuando:

- La cesión está autorizada en una ley.

- La cesión sea de datos recogidos de fuentes accesibles al público.

- La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. La comunicación

solo será legítima en cuanto se limite a la finalidad que la justifique [art. 11.2 c) LOPD y STS de 2 de junio de 2009]

- La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo[21], al Ministerio Fiscal, a los jueces o tribunales, al Tribunal de Cuentas[22], o a las ins-

21. El artículo 19.3 de la Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo, declara que "no podrá negarsele el acceso a ningún expediente o documentación administrativa o que se encuentre relacionada con la actividad o servicio objeto de la investigación". El artículo 22.1 le faculta incluso para solicitar documentos clasificados con el carácter de secretos de acuerdo con la ley. Consciente de ello, la disposición adicional quinta de la LOPD establece que "lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas".

22. Conforme al artículo 7 de la Ley Orgánica 2/1982, de 12 de mayo, el Tribunal de Cuentas puede exigir la colaboración de todas las Administraciones y entidades que integran el sector público. Estas están obligadas a suministrarle cuantos datos, estados, documentos, antecedentes o informes solicite relacionados con el ejercicio de sus funciones fiscalizadora o jurisdiccional. El incumplimiento de esta obligación puede suponer la aplicación de sanciones o el inicio de expedientes de reintegro de inversiones o gastos públicos. El Tribunal de Cuentas debe poner en conocimiento de las Cortes Generales la falta de colaboración de los obligados a presentársela.

    La sentencia de 20 de mayo de 2003, del Tribunal de Justicia de la Unión Europea, considera legítima y que, por tanto, no vulnera el derecho a la protección de datos de carácter personal, la obligación legal de las entidades públicas sujetas al control del Tribunal de Cuentas austríaco de comunicar a éste las retribuciones y pensiones superiores a un nivel deterninado, que tales entidades abonan a sus empleados y pensionistas, así como el nombre de los beneficiarios, con el objeto de elaborar un informe anual que ha de trasladarse al Parlamento nacional y a los Parlamentos de los Länder y ponerse a disposición del público en general en su informe.

    El Tribunal razona que, para controlar la buena utilización de los fondos públicos, el Tribunal de Cuentas y las asambleas parlamentarias necesitan conocer el importe de los gastos afectados a los recursos humanos en las distintas entidades públicas, y añade que "a ello se suma en una sociedad democrática, el derecho de los contribuyentes y de la opinión pública en general a ser informados de la utilización de los ingresos públicos, especialmente en materia de gastos de personal. Tales datos, reunidos en el informe, pueden contribuir al debate público relativo a una cuestión de interés general y sirven, por tanto, al interés público". El Tribunal considera que esta injerencia recogida en una ley puede justificarse solo, en la medida en que la amplia divulgación del importe de los ➢

tituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas[23], y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

Afirma la STS de 7 de noviembre de 2009 que esta "excepción sólo se predica de comunicaciones de datos con los concretos destinatarios que se indican y en el ejercicio de sus funciones, lo que necesariamente implica una comunicación directa y que la misma se produzca a requerimiento del destinatario en el ejercicio de sus funciones, circunstancias que ha de valorar el responsable del fichero para emitir la correspondiente comunicación de datos al amparo de dicha excepción, que, además y por su propia naturaleza, ha de interpretarse en sentido estricto".

Esta misma sentencia aclara que no cabe extender este supuesto excepcional "a la utilización de tales datos personales por los letrados intervinientes en determinados procesos judiciales a la hora de formular y proponer sus pruebas, concretamente los pliegos de posiciones presentados por las entidades aseguradoras, de manera que no se trata de una

➢ ingresos anuales, cuando estos superan un límite determinado, de las personas empleadas por entidades sujetas al control del Tribunal de Cuentas, y los nombres de los beneficiarios de dichos ingresos, sea a la vez necesaria y apropiada para lograr los objetivos de mantener los salarios dentro de unos límites razonables y asegurar una buena gestión de los recursos públicos.

23. El artículo 502.2 del Código Penal tipifica como delito la obstaculización por autoridad o funcionario de la investigación del Defensor del Pueblo, Tribunal de Cuentas u órganos equivalentes de las Comunidades Autónomas, negándose o dilatando indebidamente el envío de ls informes que estos soliciten o dificultando su acceso a los expedientes o documentación administrativa necesaria para tal investigación.

comunicación de datos dirigida al Juez ni a la solicitud de este en el ejercicio de sus funciones, aun cuando hubiera sido a instancia de parte, sino que, en su caso, la comunicación de los datos se dirigió a otros destinatarios distintos de los establecidos en el referido art. 11.2.d) de la LOPD y para la utilización en defensa de sus propios intereses, aun cuando ello se produjera en distintos procesos judiciales, sin que a tal efecto pueda confundirse la finalidad del uso de tales datos en el proceso, lograr la convicción del Juez en relación con los hechos que se pretenden acreditar, con el destinatario de la cesión de los datos que evidentemente no era el Juez sino aquellos que se sirvieron de ellos en defensa de sus propios intereses en tales procesos y sin que el hecho de que se admita una prueba legitime la actuación de los mismos en su proposición que no se ajuste al ordenamiento jurídico".

- La cesión sea de datos de carácter personal relativos a la salud y resulte necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

- La comunicación se realice entre Administraciones públicas para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

- La cesión se produzca entre Administraciones públicas y los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

- La cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos[24].

- La comunicación se refiera a datos tributarios para su control por la Hacienda.

La Ley General Tributaria (Ley 58/2003, de 17 de diciembre) establece, en su artículo 93, la obligación de las personas físicas o jurídicas, públicas o privadas, de proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes con trascendencia tributaria relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas. Esta obligación ha de cumplirse en los plazos que se fijen o mediante requerimiento individualizado de la Administración tributaria. El incumplimiento de la obligación no puede ampararse en el secreto bancario.

Por otro lado, el artículo 94 desarrolla el deber de todas las autoridades de suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos. A estas mismas obligaciones quedan sujetos los partidos políticos, sindicatos y asociaciones empresariales, e incluso los juzgados y tribunales, respetando estos últimos el secreto de las diligencias sumariales.

24. Como pone de manifiesto la sentencia de 16 de diciembre de 2008, del Tribunal de Justicia de la Unión Europea, el tratamiento posterior de los datos con fines estadísticos requiere que la información sea anónima, es decir, no nominativa.

La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a estos dos artículos o a otras normas de rango legal, no requiere consentimiento del afectado (artículo 94.5 LGT).

El artículo 95 de la LGT establece el carácter reservado de los datos, informes y antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones. Tales datos solo pueden utilizarse para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de sanciones, sin que pueda cederse o comunicarse a terceros. Sin embargo, cabe la cesión a órganos judiciales, otras Administraciones tributarias, Inspección de Trabajo, Seguridad Social, otras Administraciones para la lucha contra el fraude, comisiones parlamentarias de investigación, Ministerio Fiscal, Tribunal de Cuentas y otros órganos y entidades de Derecho público que se indican para finalidades determinadas.

Finalmente, por lo que se refiere a la cesión de datos entre Administraciones tributarias, el TS recuerda que "si bien el art. 113 de la Ley General Tributaria, redacción dada por la Ley 25/1995, de 20 de julio, permite tal cesión de datos a otras Administraciones Tributarias, no es menos cierto que no se trata de una cesión incondicional, sino que tiene un carácter finalista en cuanto la cesión ha de producirse a efectos de cumplimiento de las obligaciones fiscales en el ámbito de sus competencias, lo que no es sino una especificación de la previsión general del citado art. 1 de la LOPD , que limita la comunicación o cesión de datos al cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, de manera que no siendo la comunicación incondicional la concre-

ción de identificación del cesionario, en su caso el órgano administrativo, puede constituir un elemento necesario de la información a efectos de comprobar la adecuación a la ley de la cesión de datos, como es el caso de la comunicación genérica a una Administración Pública tal que una Comunidad Autónoma o Diputación Provincial de amplias competencias no limitadas al ámbito tributario, cuya omisión priva al interesado de tal comprobación, limitando con ello el ejercicio del derecho de información que le reconoce la Ley".

Sin embargo, los supuestos que cita el art. 11.2 de la LOPD no pueden considerarse los únicos posibles de comunicación de datos personales sin consentimiento previo. Existen otros, sobre todo, los relacionados con la libertad de información o con el deber de información de los poderes públicos que admiten más supuestos. Así, por ejemplo, la STS 19 octubre 2011 considera que no vulnera el derecho a la protección de datos de carácter personal la simple y objetiva información facilitada por una Administración a los medios de comunicación locales, de la incoación y de la posterior resolución de un expediente sancionador a un funcionario, sin ningún otro añadido ni comentario ajeno a los mencionados hechos. Ha de considerarse como un medio razonable e idóneo para cumplir el deber de información de la Administración sobre sus actos, que es una finalidad querida por las normas que disciplinan la actuación de los entes públicos (STS 19 de octubre de 2011). Añade esta sentencia que "asimismo, tal comunicación de los actos administrativos de incoación de un expediente o de su resolución igualmente aparece como una vía razonable y moderada para la consecución del fin propuesto y, por último, de esta comunicación se derivan los beneficios o ventajas para el interés general del conocimiento por los ciudadanos de la actuación ad-

ministrativa, a la vista además de la trascendencia social que tuvieron los hechos en la localidad, por la materia y las personas intervinientes, que justifican los perjuicios sufridos por el derecho a la protección de datos del recurrente, que han de considerarse mínimos, en atención a que los datos que se reputan revelados, que se refieren todos ellos a actos del funcionario del Ayuntamiento en tal condición y a actos del Ayuntamiento también en la esfera de sus funciones administrativas".

El proyecto de Reglamento General de Protección de Datos ya contempla en su artículo 80 la posibilidad para los Estados miembros de exencionar de la mayor de la legislación sobre protección de datos "en lo referente al tratamiento de los datos personales efectuado exclusivamente con fines periodísticos o de expresión literaria o artística, para conciliar el derecho a la protección de los datos de carácter personal con las normas que rigen la libertad de expresión".

También este proyecto de Reglamento General contiene normas especiales para los casos del tratamiento de los datos personales de los trabajadores en el ámbito laboral, en particular para la contratación de personal, la ejecución del contrato laboral, la organización del trabajo, la salud y la seguridad en el trabajo, así como a los fines del ejercicio y disfrute de los derechos y prestaciones relacionados con el empleo y a efectos del cese de la relación laboral (art. 82).

También las Leyes de Transparencia que se van aprobando por las Comunidades Autónomas, o la que se apruebe por las Cortes Generales, contemplan supuestos de información de datos personales sin consentimiento previo del afectado.

Los requisitos del consentimiento. El consentimiento nulo.

Volviendo al consentimiento, la solicitud de este que se haga al interesado debe ir referida a un tratamiento o cesión concreta, con delimitación de la finalidad para el que se recaba o cede, así como de las restantes condiciones que concurran en el tratamiento o cesión, incluido el tipo de actividad desarrollada por el cesionario. En caso contrario, la Ley considera nulo el consentimiento.

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

Es válido el consentimiento de los mayores de 14 años (salvo cuando la ley exija la asistencia de los titulares de la patria potestad o tutela), pero, para los menores de esa edad, se requiere el consentimiento de los padres o tutores.

El consentimiento se entiende otorgado si, una vez informado el afectado y concedido un plazo de treinta días hábiles para manifestar su negativa, esta no se manifiesta. Es una muestra más del consentimiento tácito.

El consentimiento puede ser revocado cuando exista causa justificada para ello. A esta revocación no se le atribuyen efectos retroactivos. El responsable debe cesar en el tratamiento de los datos en el plazo máximo de diez días a contar desde la recep-

ción de la revocación del consentimiento. Si los datos han sido cedidos, el responsable, una vez revocado el consentimiento, debe comunicarlo a los cesionarios en el plazo máximo de diez días, para que estos cesen en el tratamiento de los datos.

Aquel a quien se comunican los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la LOPD.

Si la comunicación se efectúa previo procedimiento de disociación, es decir, si el dato no permite la identificación del afectado o interesado, no es aplicable lo establecido en los puntos anteriores.

Es importante destacar que la Ley no considera comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento (art. 12.1 LOPD y SSTS de 16 de septiembre, 9 de octubre y 14 de octubre de 2009).

Para el TS, el art. 12.1 de la LOPD "pone de manifiesto, con incuestionable claridad que el legislador, precisamente con el objeto de garantizar y proteger las libertades públicas, y especialmente de su honor e intimidad personal y familiar, en el ámbito correspondiente al tratamiento de los datos personales, -objeto descrito en el artículo 1- ha querido excluir del concepto de comunicación de datos aquellos supuestos en que el acceso de un tercero a los mismos venga exigido para la prestación de un servicio al responsable del tratamiento, pero ninguno más". Así, el Tribunal excluye de la cobertura del precepto los contratos de colaboración entre empresas, en que las partes se com-

prometen a un objeto que va más allá del servicio del de tratamiento de datos y persiguen el "desarrollo de sus respectivos negocios, en beneficio de ambas partes" y "tratan de fomentar e incrementar sus respectivos volúmenes de negocios" (STS de 9 de octubre de 2009).

Por el contrario, el TS considera que encaja en este precepto un contrato entre dos empresas para la prestación de servicios de gestión comercial de la cartera de clientes relacionados con el suministro de energía eléctrica y otras actividades conexas con dicho suministro, cuando, además, no se incluye en el objeto ningún otro tipo de actividades o servicios (STS de 16 de septiembre de 2009).

La realización de tratamientos por cuenta de terceros debe estar regulada en un contrato, que debe constar por escrito o en alguna otra forma que permita acreditar su celebración (art. 12.2 LOPD y STS de 30 de enero de 2012) y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con el fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas (véanse las SSTS de 27 de marzo de 2007, 6 de mayo de 2008 y 14 de octubre de 2009).

Conforme a una amplia jurisprudencia, los requisitos que deben concurrir para que no se considere comunicación de datos el acceso de un tercero a los datos para la prestación de un servicio al responsable del tratamiento son: "En primer lugar, el responsable del fichero debe haber encomendado el tratamiento de los datos mediante un contrato, pactado de forma que permita comprobar

su existencia así como su contenido. En segundo término, dicha convención ha de contener las instrucciones que el responsable del tratamiento impone para el uso de los datos y de los que el encargado no puede separarse. Finalmente, tiene que constar también el fin que legitima la comunicación, que no pueden obviar las partes, quienes, además, han de abstenerse de comunicar los datos a otras personas" (por todas, SSTS de 4 de mayo, 29 de junio y 14 de octubre de 2009 y 17 de septiembre de 2010).

Si no concurren las condiciones legales que exige el art. 12.2 de la LOPD, no puede sostenerse que haya habido prestación de un servicio al responsable del tratamiento y, por consiguiente, debe considerarse comunicación que requiere consentimiento del interesado (STS de 28 de abril de 2009).

Por su parte, la STS de 4 de mayo de 2009, considera que "el artículo 12 de la Ley Orgánica 15/1999 constituye una unidad, sin que resulte lícito separar sus distintos apartados como si de compartimentos estancos se tratara. De este modo, para que no se considere comunicación de datos el acceso de un tercero a los mismos en el seno de un servicio que ha de prestar al responsable del tratamiento, han de cumplirse las exigencias recogidas en el apartado 2. Dicho de otra forma, si un tercero tiene a su alcance los datos para rendir un servicio al responsable del tratamiento, pero lo hace sin previo contrato en el que conste de forma inequívoca las instrucciones a las que ha de ajustarse u opera al margen o con incumplimiento del mismo, ese acceso tiene la consideración de comunicación y queda sometido al régimen general, esto es, a la necesidad de consentimiento del interesado, conforme dispone el artículo 11 de la propia Ley Orgánica 15/1999".

En el contrato se han de estipular, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

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

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

C. El principio de veracidad del dato.

Este principio se traduce en que los datos de carácter personal que figuren en un fichero han de ser exactos, completos y actuales (art. 4.3 LOPD y STS de 29 de marzo de 2011).

Se presumen exactos los datos facilitados directamente por el afectado.

El responsable o el encargado están obligados a ponerlos al día de forma que respondan con veracidad a la situación actual del afectado. Esta actualización de los datos no requiere comunicación alguna al interesado.

Este principio tiene sus consecuencias, pues si los datos de carácter personal registrados resultan ser inexactos, en todo o en

parte, o incompletos, el responsable o el encargado ha de cancelarlos y sustituirlos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hayan sido comunicados previamente, el responsable del fichero o tratamiento debe notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantenga el tratamiento de los datos, debe proceder a la rectificación o cancelación notificada.

Todo lo anterior lo es sin perjuicio de las facultades que a los afectados reconoce la LOPD de cancelación o rectificación, y que se exponen más adelante.

D. El principio de licitud del dato.

El tratamiento ha de ser realizado de formal leal y lícita. Esto es tanto como decir que está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos, y si así se hace, el fichero será ilegal.

Se considera un tratamiento lícito cuanto "es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos" (sentencia del 16 de diciembre de 2008, del Tribunal de Justicia de la

Unión Europea), o "si es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento (sentencia de 20 de mayo de 2003, del mismo Tribunal).

E. Principio de acceso al dato.

Conforme a este principio, los datos de carácter personal deben estar almacenados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda legalmente su cancelación.

F. Principio de vida útil del dato.

Conforme a este principio, 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.

Por tanto, no deben ser conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados[25]. No obstante, los datos pueden conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Así, por ejemplo, hemos visto que las imágenes de videovigilancia tienen una vida útil de treinta días.

25. Véase al respecto la sentencia del Tribunal de Justicia de la Unión Europea de 7 de mayo de 2009.

Excepcionalmente, puede acordarse el mantenimiento íntegro de tales datos atendiendo a los valores históricos, estadísticos o científicos que contienen de acuerdo con la legislación específica.

4. LOS DATOS PERSONALES ESPECIALMENTE PROTEGIDOS.

La LOPD diferencia los datos personales normales de los datos que llama "especialmente protegidos" o sensibles.

Son datos especialmente protegidos los relacionados con: la ideología, la religión, las creencias (SSTS de 19 de septiembre de 2008, sobre Libros de Bautismo, y 10 de noviembre de 2011, sobre cancelación de datos de una asociación religiosa), la afiliación sindical, el origen racial, la vida sexual y la salud.

a) De entrada, nadie puede ser obligado a declarar sobre los datos referidos a su ideología, religión o creencias. Se trata de una concreción del derecho o libertad que reconoce a cualquier persona el artículo 16.2 de la Constitución: "Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias".

Además, cuando, se proceda a recabar el consentimiento de datos sobre las ideas de una persona, ha de advertirse al interesado que tiene derecho a no prestar el consentimiento.

En lo relacionado con estos datos personales, el consentimiento del afectado ha de ser personal, expreso y constar por escrito. No se aplica, por tanto, la regla del consentimiento tácito, que sí cabe en los datos ordinarios.

No obstante, se exceptúan de las reglas que figuran en este apartado los ficheros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros (relaciones *ad intra*, por ser asumida voluntariamente). Pero la cesión de estos datos a un tercero ajeno de ese grupo al que voluntariamente se ha decidido pertenecer (relaciones *ad extra*) precisa "siempre el previo consentimiento del afectado".

b) Los datos de carácter personal que hacen referencia al origen racial, a la salud y a la vida sexual. Por su trascendencia en la vida de las personas y el riesgo que conlleva su uso con fines discriminatorios, tales datos solo pueden ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art. 7.3 LOPD y SSTS de 23 de enero y 5 de marzo de 2012).

La LOPD prohíbe tajantemente los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas solo pueden ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. No cabe la existencia de ficheros de particulares al respecto, ni tampoco de otras Administraciones que no sean las estrictamente competentes. El próximo reglamento comunitario

sobre la protección de datos personales plantea considerar expresamente los datos referidos a infracciones personales o administrativas como especialmente sensibles.

Datos relacionados con la salud.

La información sobre la salud juega un papel fundamental para el ejercicio del derecho al respeto de la vida privada y familiar. El Tribunal Europeo de Derechos Humanos ha declarado que "el respeto del carácter confidencial de la información sobre la salud constituye un principio esencial del sistema jurídico" relativo a la protección de los datos personales, y ha añadido que "es muy importante no sólo para proteger la vida privada de los enfermos sino también para preservar su confianza en el cuerpo médico y los servicios de salud en general. En ausencia de dicha protección, las personas que necesitan cuidados médicos podrían se disuadidas de ofrecer información de carácter personal e íntima necesaria para la prescripcion del tratamiento apropiado, incluso consultar a un médico, lo que podría poner en peligro su salud y, por tanto, en caso de enfermedades de transmisión, la de la colectividad" (sentencias de 25 de febrero de 1997, 17 de junio de 2008 y 6 de octubre de 2009).

Para este Tribunal, se produce una violación del derecho a la vida privada cuando se permite el acceso no autorizado, en un sistema hospitalario, al historial médico, por personas no directamente involucradas en el tratamiento médico del paciente (sentencia de 17 de julio de 2008). E, igualmente, hay violación de este derecho, cuando una sentencia de un órgano judicial divulga la identidad del demandante y su enfermedad, tras ser solicitada su eliminación o sustitución por iniciales (sentencia de 6 de octubre de 2009)

Lo dicho no obsta para que, como ya se ha apuntado, estos datos especialmente protegidos sí puedan ser objeto de tratamiento, cuando este resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También pueden ser objeto de tratamiento los datos especialmente sensibles cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes pueden proceder al tratamiento de los datos relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, si bien dicho tratamiento ha de hacerse de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

El art. 10.5 del RPDP aclara, con cierta lógica, que no es necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud, pero siempre que la cesión se realice para la atención sanitaria de las personas, conforme a la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

Por otro lado, el Tribunal de Justicia de la Unión Europea califica el hecho de que una persona se haya lesionado y esté en situación de baja parcial como un dato personal relativo a la salud y , por tanto, especialmente sensible a efectos de su protección. Para este Tribunal, debe darse una interpretación amplia a la expresión "datos relativos a la salud", de modo que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona (sentencia de 6 de noviembre de 2003).

Por su parte, la STS de 5 de marzo de 2012 considera que "el sólo dato de la fecha de baja, sin ningún otro añadido o explicación, no puede considerarse como dato de salud". Para el TS, "el artículo 7.3 de la LOPD se refiere a los datos de salud para considerarlos especialmente protegidos, limitando la posibilidad de recabar, tratar y ceder tales datos a los casos en los que lo disponga una ley o el afectado consiente expresamente, pero no delimita el concepto de dato de salud. El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa (Estrasburgo, 28.I.1981), para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, considera que los datos de carácter personal relativos a la salud abarcan las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. Añade el citado apartado que la información puede referirse a una persona de buena salud, enfermo o fallecido y que debe entenderse que esta categoría de datos también comprenden aquellos relativos al abuso de alcohol o al consumo de drogas. También en el ámbito del Consejo de Europa, la Recomendación R (97) 5, adoptada por el Comité de Ministros del 13 de febrero de 1.997, señala que la expresión datos médicos hace referencia a todos

los datos de carácter personal relativos a la salud de una persona y afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas. Tales conceptos han tenido acogida en el Reglamento de desarrollo de la LOPD, que en su artículo 5.1, letra g) define los datos de carácter personal relacionados con la salud como las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo, y, en particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética".

La STS de 23 de enero de 2012 aclara que los datos personales "tales como el nombre, apellidos, número de teléfono y fecha de la baja laboral (…) no pueden considerarse datos personales de salud, especialmente protegidos por el artículo 7.3 LOPD, que requieren consentimiento expreso del titular para ser cedidos", aunque sí " por disposición del artículo 6.1 LOPD, el consentimiento del afectado ha de ser inequívoco ".

5. LOS DERECHOS DE LOS INTERESADOS RESPECTO A LOS DATOS PERSONALES QUE LES CONCIERNAN.

La LOPD reconoce a las personas un amplio catálogo de derechos respecto a sus datos personales. Son facultades que integran el superior derecho a la protección de datos personales[26], y son las siguientes:

26. Por ejemplo, la sentencia de 7 de mayo de 2009, del Tribuna de Justicia de la Unión Europea, pone en relación los derechos de acceso, rectificación, cancelación y oposición.

a) El derecho a ser informado previamente a la recogida de datos (art. 5 LOPD).

b) El derecho a impugnar actos o decisiones que impliquen una valoración de su comportamiento (art. 13 LOPD).

c) El derecho de consulta al Registro General de Protección de Datos (art. 14).

d) El derecho de acceso a sus datos de carácter personal (art. 15).

e) El derecho a la rectificación (art. 16).

f) El derecho de cancelación (art. 16).

g) El derecho de oposición.

h) El derecho a ser indemnizado por daños o lesiones sufridos como consecuencia del incumplimiento de lo dispuesto en la LOPD.

Los derechos de acceso, rectificación, cancelación y oposición son: a´) derechos personalísimos, por lo que solo pueden ser ejercicios por el afectado, directamente o mediante representante; b´) independientes entre sí; y c´) de ejercicio gratuito.

Por otro lado, el proyecto de Reglamento General de Protección de Datos reconoce como derechos del interesado los de: información, acceso a los datos, rectificación, supresión o "derecho al olvido", portabilidad de los datos, oposición, a no ser evaluada en determinados aspectos personales o profesionales, a

presentar una reclamación ante una autoridad de control, a un recurso judicial contra la autoridad de control, a un recurso judicial contra un responsable o encargado del tratamiento de los datos personales y a ser indemnizado por los perjuicios que sufra por un tratamiento ilegal.

A. El derecho a ser informado previamente a la recogida de datos.

Este derecho garantiza a todo interesado al que se le soliciten datos personales ser previamente informado de modo expreso, preciso e inequívoco. Es un deber para quien realiza el tratamiento. El interesado debe ser informado antes de la recogida:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Ahora bien, estas informaciones anteriores no son necesarias si el contenido de ellas se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando se utilicen cuestionarios u otros impresos para la recogida, han de figurar en ellos, en forma claramente legible, estas advertencias recogidas como letras a) a e).

Cuando los datos de carácter personal no hayan sido recabados del interesado, este debe ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de las demás previsiones que se han dicho.

No se aplica esta exigencia cuando:

a) una ley lo excepcione expresamente;

b) el tratamiento tenga fines históricos, estadísticos o científicos;

c) los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le debe informar del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten;

d) la información al interesado resulte imposible, o

e) exija esfuerzos desproporcionados, a criterio de la AEPD o de la autoridad autonómica equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias;

f) afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

B. El derecho de impugnación de valoraciones (art. 13).

Es el derecho del ciudadano a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

El afectado puede impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tiene derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

Esta valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente puede llegar a tener valor probatorio a petición del afectado.

C. El derecho de consulta al Registro General de Protección de Datos (art. 14).

Cualquier persona puede conocer, recabando la información oportuna del Registro General de Protección de Datos de la AEPD, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

El Registro General es de consulta pública y gratuita.

D. El derecho de acceso (art. 15).

Es el derecho del interesado a solicitar y obtener gratuitamente información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que se esté realizando, la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o que se prevé hacer de los mismos (art. 15.1 LOPD y SSTS de 7 de julio de 2009 y 11 de marzo de 2011, la primera de ambas en relación con la Agencia Tributaria).

Es un derecho distinto del derecho de acceso que otorga la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La información puede obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteli-

gible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

El responsable del fichero debe resolver sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin atenderse la solicitud, el interesado puede interponer reclamación ante la AEPD. Si se estima la solicitud, pero no se indica plazo para concretar su ejercicio, este es de diez días.

Este derecho puede denegarse en tres casos:

- En los supuestos en que lo prevea una ley.

- Si el derecho se ha ejercitado en los doce meses anteriores, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso puede ejercitarlo antes.

- Cuando una ley impide al responsable del tratamiento revelar a los afectados el tratamiento de los datos a que se refiera el acceso.

También cabe la denegación del derecho de acceso cuando se observa que el solicitante actúa en contra del principio de la buena fe. Así lo ha reconocido el TS en una amplia jurisprudencia (SSTS de 26 de enero, 2 de julio y 22 de octubre de 2010; y 4 de febrero y 18 de febrero de 2011). Para el Tribunal, resulta injustificada una solicitud de acceso a datos personales desde el momento en que el solicitante disponía ya de la posibilidad permanente de acceso a sus datos personales por vía informática. Se trata, según afirma, de una solicitud reiterativa,

meramente retórica, y el hecho de presentar luego una reclamación ante la AEPD por incumplimiento del deber de permitir el acceso a los datos personales supone comportamiento contrario a la buena fe. No es leal reprochar a otro no haber hecho algo que, en realidad, ya ha hecho. "no se trata sólo de que el solicitante dispusiera de la posibilidad permanente de acceso a sus datos personales por vía informática, sino que en su escrito no especificó mediante qué concreto medio de acceso quería que su derecho fuese satisfecho; y, en estas circunstancias, afirmar que se le denegó el acceso en el plazo legalmente previsto resulta sencillamente una abusiva deformación de la realidad". Concluye el TS señalando que "dado que el ejercicio desleal del derecho de acceso a los datos personales por el particular no es merecedor de tutela, la AEPD, en cuanto entidad administrativa encargada de velar por el cumplimiento de la legislación de protección de datos, no debió estimar que se había vulnerado el derecho del solicitante, y lo propio cabe decir del tribunal a quo, al reputar ajustada a derecho la citada decisión de la AEPD".

Por otro lado, sí que el TS ha ratificado el parecer de la Audiencia Nacional acerca del alcance de este derecho. Conforme a lo recogido en la STS de 11 de marzo de 201, las valoraciones o apreciaciones de índole médico sobre el encaje de las lesiones o secuelas padecidas por la recurrente no deben considerarse como datos de carácter personal a los que se tenga derecho de acceso. El TS hace suyas las siguientes palabras de la Audiencia Nacional: "los datos que deben proporcionarse por el cauce del derecho de acceso son todos aquellos datos relativos a la determinación y constatación de sus lesiones, su evolución y, en su caso, las secuelas advertidas, que afectan a la salud de la ti-

tular de los datos, pero no pueden incluirse, como datos de base, las valoraciones o apreciaciones de índole médica sobre el encaje de las lesiones o secuelas padecidas en la aplicación del baremo del Real Decreto Legislativo 8/2004". Se desvinculan así de los datos de carácter personal, "las apreciaciones que se refieren a las consecuencias económicas derivadas de las lesiones y, en todo caso, no vinculadas a la salud de la titular de los datos denunciante". Para la Audiencia Nacional, en la sentencia objeto de casación, "estas apreciaciones y valoraciones realizadas por un médico, partiendo de los datos de base que proporciona la exploración y la documentación facilitada por la propia denunciante ante la Agencia, obran en poder de la parte recurrente, como responsable del fichero, que realiza un encargó a un profesional de la medicina para la elaboración de un informe médico. Pues bien, la operación intelectual, de carácter técnico -por aplicación de conocimientos médicos-, en virtud de la cual las lesiones o secuelas encajan en los diferentes apartados del baremo, no puede integrase en la categoría de <<datos de base>>, del artículo 13 del citado Real Decreto 1332/1994, pues nos encontramos ante estimaciones de orden técnico propias de un experto, en este caso, en medicina, al que se le encarga un trabajo de evaluación médica. Su contenido, en esta parte, por tanto, excede de lo que ha de incluirse en la información como <<datos de base>>, pues no se integran por referencias a los datos del titular, sino que reflejan apreciaciones de un profesional de la medicina, relacionadas no con la salud de la titular de los datos sino con las repercusiones económicas que pudieran tener sus dolencias".

El Tribunal de Justicia de la Unión Europea ha recordado el deber de los Estados miembros de la Unión de garantizar "a

todos los interesados un derecho de acceso a los datos personales que le conciernen, así como información sobre los destinatarios o las categorías de los destinatarios a quienes se comuniquen dichos datos, sin establecer un plazo concreto". Considera que este derecho es indispensable para ejercer otros derechos, como los de rectificación, supresión o bloqueo de datos, oposición al tratamiento o a recurrir por los daños sufridos (sentencia de 7 de mayo de 2009). Aborda, además, el problema de cuál es la extensión o plazo del citado derecho en el pasado, concluyendo que corresponde a los Estados miembros fijar un plazo que no debe ser superior al necesario para los fines para los que los datos fueron recogidos o para lo que se traten ulteriormente considerando el plazo de un año como plazo general excesivo.

E. Los derechos de rectificación y cancelación (art. 16).

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

El derecho de cancelación es el derecho que da lugar a que se supriman los datos que resulten ser inadecuados o excesivos o que no se ajusten a la LOPD, sin perjuicio del deber de bloqueo.

La solicitud de rectificación o cancelación debe indicar los datos a que se refiere y, en su caso, la corrección, aportando la documentación justificativa.

El responsable del fichero tiene la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el

plazo de diez días (art. 16.1 LOPD y STS de 10 de noviembre de 2011). Transcurrido el plazo sin respuesta, puede acudir en reclamación a la AEPD.

La cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, jueces y tribunales de justicia, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de estas. Cumplido el citado plazo, debe procederse a la supresión.

Si los datos rectificados o cancelados han sido comunicados previamente, el responsable del tratamiento debe notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que debe también proceder a la cancelación.

Los datos de carácter personal deben ser conservados durante los plazos previstos en las disposiciones aplicables[27] o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

F. El derecho de oposición.

Es el derecho del afectado a que no se lleve el tratamiento de sus datos personales o se cese en ese tratamiento.

27. Resulta interesante la sentencia de 7 de mayo de 2009, del Tribunal de Justicia de la Unión Europea. En ella, el Tribunal considera que vulnera el derecho a la protección de datos personales la normativa que limita la conservación de la información sobre los destinatarios y el contenido de los datos al período de un año, limitando correlativamente el acceso a dicha información, si bien los datos principales se conservan durante mucho más tiempo.

Se puede ejercer en los tres siguientes supuestos:

a) Cuando no sea necesario el consentimiento del afectado para su tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

El derecho ha de ejercerse mediante solicitud dirigida al responsable del tratamiento. Este tiene diez días para resolver la solicitud. Transcurrido el plazo sin que se responda expresamente, el interesado puede interponer reclamación ante la AEPD. El responsable tiene diez días para excluir el tratamiento o denegar la solicitud.

La regulación del derecho de oposición en la LOPD es francamente deficitaria, como han puesto de manifiesto la Audiencia Nacional (sentencia de 6 de junio de 2007) y el Tribunal Supremo (STS de 14 de abril de 2011). Ambos órganos judiciales criticaron con dureza la regulación fragmentaria e incompleta del derecho de oposición en la LOPD, así como el retraso del

Gobierno en su regulación reglamentario. Negaron también la aplicación analógica del derecho de acceso a este derecho específico, así como las referencias a la Directiva 95/46/CE, por ya estar esta transpuesta al ordenamiento jurídico español por la LOPD. De ahí que, en consecuencia, negaran la posibilidad de ejercitar este derecho hasta su regulación en los arts. 34 a 36 del Reglamento de la LOPD, como hoy puede hacerse.

El art. 19 del proyecto de Reglamento General de Protección de Datos reconoce este derecho al interesado para oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales sean objeto de un tratamiento. No obstante, el responsable del tratamiento puede alegar y acreditar motivos imperiosos y legítimos para que el tratamiento prevalezca sobre los intereses y derechos del interesado. El derecho de oposición jugará con más fuerza en la mercadotecnia directa, en donde el interesado tendrá derecho a oponerse sin que ello le suponga gasto alguno al tratamiento de sus datos personales. El ejercicio del derecho obliga al responsable del tratamiento a dejar de usar o tratar de cualquier otra forma los datos personales en cuestión.

G. El derecho a indemnización (art. 19).

Es el derecho de los que, como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento, sufren un daño o una lesión en sus bienes o derechos, a ser indemnizados.

Cuando se trata de ficheros de titularidad pública, la responsabilidad se ha de exigir de acuerdo con la legislación reguladora

del régimen de responsabilidad de las Administraciones públicas, que hoy se encuentra en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

En el caso de los ficheros de titularidad privada, la acción se ha de ejercitar ante los órganos de la jurisdicción ordinaria.

H. La tutela de estos derechos: la reclamación ante la AEPD (art. 18).

El artículo 18 de la LOPD otorga a la AEPD la tutela de los derechos de las personas en lo relacionado con sus datos personales. Conforme a este precepto legal, el interesado puede reclamar contra cualquier actuación contraria a lo dispuesto en la LOPD ante la Agencia Española de Protección de Datos.

También, a quien se le deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, puede ponerlo en conocimiento de la AEPD o, en su caso, de la autoridad equivalente de la Comunidad Autónoma, que ha de asegurarse de la procedencia o improcedencia de la denegación.

Los artículos 117 a 119 del Reglamento de la LOPD especifican el procedimiento de tutela de tales derechos de acceso, rectificación, cancelación y oposición.

Aclara la STS de 19 de mayo de 2010 que esta reclamación ante la AEPD es una simple facultad y no una obligación del interesado que no ve atendido su derecho de acceso, rectificación, cancelación u oposición.

El plazo máximo en que la AEPD o la autoridad autonómica equivalente debe dictar la resolución expresa de tutela de derechos es de seis meses. Durante ese plazo, tiene que oírse al responsable del fichero para que formule las alegaciones que estime pertinentes en el plazo de quince días. Transcurrido el plazo de seis meses sin notificarse resolución expresa, el afectado puede considerar estimada la reclamación por silencio administrativo positivo.

Si la resolución es estimatoria, se ha de requerir al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la AEPD en idéntico plazo.

Contra las resoluciones de la AEPD procede recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

6. DEBERES DEL RESPONSABLE O ENCARGADO DEL FICHERO.

El responsable del fichero o el encargado del tratamiento tienen estos deberes:

A. De seguridad de los datos (art. 9 LOPD).

Este deber le obliga a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de

la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Este deber conlleva que no se pueden registrar datos de carácter personal en ficheros que no reúnan las condiciones que se determinen con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

B. De secreto (art. 10).

Obliga a guardar el secreto profesional respecto de los datos. La obligación subsiste aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. El deber se extiende a cualquier persona que intervenga en cualquier fase del tratamiento de los datos.

Este deber pretende que los datos personales no puedan conocerse por terceros, salvo de acuerdo con los preceptos de la LOPD (STS de 10 de junio de 2011). Trata de salvaguardar y tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal. Está relacionado con el deber de secreto profesional, al que el TC concibe como "la sustracción al conocimiento ajeno, justificada por razón de una actividad, de datos o informaciones obtenidas que conciernen a la vida privada de las personas" (ATC 600/1989, de 11 de diciembre).

7. FICHEROS DE TITULARIDAD PÚBLICA.

A. Creación, modificación o supresión (art. 20).

La creación, modificación o supresión de los ficheros de las Administraciones públicas solo puede hacerse por medio de una disposición general publicada en el BOE o en el Diario Oficial correspondiente.

Las disposiciones de creación o de modificación de ficheros deben indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

En las disposiciones que se dicten para la supresión de los ficheros, se ha de establecer el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

B. Comunicación de datos entre Administraciones públicas (art. 21).

Principio general: Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no pueden comunicarse a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, sin consentimiento del interesado.

Dicho de otro modo, la comunicación de los datos entre Administraciones para el ejercicio de competencias entre las mismas materias no requiere consentimiento del interesado.

Excepciones: se exceptúa del principio general (y, por tanto, tampoco en estos casos se hace necesario el consentimiento del interesado) la comunicación:

a) Que tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

b) De datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

c) De datos recogidos de fuentes accesibles al público. Sin embargo, la comunicación a ficheros de titularidad privada no puede hacerse sin el consentimiento del interesado o cuando una ley no lo prevea.

Conviene recordar que la STC 292/2000, de 30 de noviembre, declaró inconstitucional la excepción prevista en la LOPD en los casos de comunicación que *hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso*. El Tribunal Constitucional exige que el consentimiento sea del interesado o esté exceptuado por una norma con rango de ley.

C. Ficheros de las Fuerzas y Cuerpos de Seguridad (art. 22).

Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal para fines administrativos y deban ser objeto de registro permanente, están sujetos a la LOPD.

La LOPD declara que cabe la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, en los supuestos y categorías de datos que resultan necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales[28].

28. El Tribunal de Justicia de la Unión Europea declara legítimo el uso por la policía, o por la Administración, de un Registro de Extranjeros residentes en Alemania, como medio de apoyo para las autoridades encargadas de aplicar la normativa en materia de derecho de residencia, y lo considera compatible con la prohibición de discriminación por razón de la nacionalidad. No obstante, declara también que "un Registro de ese tipo no podrá contener más información que la que resulte necesaria al mencionado fin", y que debe ser actualizado, debiendo cancelarse los datos superfluos (sentencia de 16 de diciembre de 2008).

Estos datos deben ser almacenados en ficheros específicos establecidos al efecto, que deben clasificarse por categorías en función de su grado de fiabilidad.

La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos especialmente protegidos puede realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

Los datos personales registrados con fines policiales han de cancelarse cuando no sean ya necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se ha de tener en consideración especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Es importante destacar que la LOPD faculta a los responsables de estos ficheros policiales para denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para: a) la defensa del Estado o la seguridad pública; b) la protección de los derechos y libertades de terceros, o c) las necesidades de las investigaciones que se estén realizando.

D. La base de datos policial sobre identificadores obtenidos a partir del ADN.

La Ley Orgánica 10/2007, de 8 de octubre, regula la base de datos policial de identificadores obtenidos a partir del ADN. Esta Ley se inscribe expresamente en el marco de la LOPD, la

cual resulta de aplicación directa, siendo los preceptos de la LO 10/2007 especificidades de la regulación general contenida en la LOPD (disposición adicional segunda).

La Ley crea la base de datos policial de identificadores obtenidos a partir del ADN, que integra los ficheros de esta naturaleza de titularidad de las Fuerzas y Cuerpos de Seguridad del Estado, tanto para la investigación y averiguación de delitos, como para los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas (art. 1). Esta base depende del Ministerio del Interior (art. 2).

Se inscriben en la base los siguientes datos:

a) Los datos identificativos extraídos a partir del ADN de muestras o fluidos que, en el marco de una investigación criminal, hayan sido hallados u obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada.

b) Los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desconocidas.

La inscripción en esta base de datos no precisa el consentimiento del afectado. Sin embargo, este debe ser informado por

escrito de todos los derechos que le asisten respecto a la inclusión en la base, quedando constancia de ello en el procedimiento. También pueden inscribirse los datos identificativos obtenidos a partir del ADN cuando el afectado haya prestado expresamente su consentimiento.

Ahora bien, solo pueden inscribirse en esta base de datos los identificadores obtenidos a partir del ADN, en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo (art. 4).

Los datos contenidos en esta base de datos solo pueden utilizarse por las unidades de la Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado. Los datos pueden cederse a: a) las autoridades judiciales, fiscales o policiales de terceros países, de acuerdo con lo previsto en los convenios internacionales vigentes; b) a las policías autonómicas con competencia estatutaria para la protección de personas y bienes y para el mantenimiento de la seguridad pública, que, a su vez, únicamente pueden utilizar los datos para la investigación de los delitos o, en su caso, para la identificación de cadáveres o averiguación de personas desaparecidas; y c) al Centro Nacional de Inteligencia.

Todos los ficheros están sometidos al nivel de seguridad alto, de acuerdo con la LOPD.

La conservación de los identificadores obtenidos a partir del ADN en la base de datos no puede superar el tiempo señalado en la Ley para la prescripción del delito, ni el tiempo señalado en la Ley para la cancelación de antecedentes penales, si se hu-

biese dictado sentencia condenatoria firma, o absolutoria por la concurrencia de causas eximentes por falta de imputabilidad o culpabilidad, salvo resolución judicial en contrario.

Procede la cancelación cuando se haya dictado auto de sobreseimiento libre o sentencia absolutoria por causas distintas de las mencionadas en el punto anterior, una vez que sean firmes dichas resoluciones. En el caso de sospechosos no imputados, la cancelación de los identificadores inscritos se ha de producir transcurrido el tiempo señalado en la Ley para la prescripción del delito.

En los supuestos en que en la base de datos existan diversas inscripciones de una misma persona, correspondientes a diversos delitos, los datos y patrones identificativos inscritos se han de mantener hasta que finalice el plazo de cancelación más amplio.

Los datos pertenecientes a personas fallecidas han de cancelarse una vez el encargado de la base de datos tenga conocimiento del fallecimiento.

El ejercicio de los derechos de acceso, rectificación y cancelación en relación con esta base de datos se sujeta a la LOPD.

Por lo que respecta a la toma de muestra y fluidos del sospechoso, detenido o imputado, así como del lugar del delito, esta de hacerse por la policía judicial en el marco de la investigación de los delitos. En todo caso, la toma de muestras que requieran inspecciones, reconocimientos o intervenciones corporales, sin consentimiento del afectado, precisa autorización judicial mediante auto motivado (disposición adicional tercera).

E. Ficheros de Hacienda.

Los responsables de los ficheros de la Hacienda Pública pueden denegar el ejercicio de los derechos de acceso, rectificación o cancelación, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

La Instrucción 6/2000, de la Agencia Estatal de la Administración Tributaria, regula el ejercicio de los derechos de acceso, rectificación y cancelación de sus ficheros automatizados.

F. Revisión por el Director de la AEPD.

El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados, puede ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma (en el caso de ficheros mantenidos por Cuerpos de Policía propios de estas, o por las Administraciones tributarias autonómicas), quienes deben asegurarse de la procedencia o improcedencia de la denegación.

G. Ficheros y Registros de Población de las Administraciones públicas.

La Administración General del Estado y las Administraciones de las Comunidades Autónomas pueden solicitar al Instituto Nacional de Estadística (INE), sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre,

apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

Los ficheros o registros de población tienen como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las Administraciones públicas.

H. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no pueden ser consultados, salvo que:

a) Medie consentimiento expreso de los afectados, o

b) Hayan transcurrido cincuenta años desde la fecha de aquéllos. En este supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, ha de poner a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

8. FICHEROS DE TITULARIDAD PRIVADA.

A. Creación (art. 25).

Para que puedan crearse ficheros de titularidad privada que contengan datos de carácter personal, han de cumplirse conjuntamente dos requisitos:

a) Que resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular, y

b) Que se respeten las garantías que la LOPD establece para la protección de las personas.

Es decir, solo puede crearse un fichero de titularidad privado cuando se respete el principio de finalidad legítima y con arreglo a la Ley.

B. Notificación e inscripción registral (art. 26).

La persona o entidad que proceda a la creación de ficheros de datos de carácter personal tiene el deber de notificarlo previamente a la AEPD.

La notificación ha de contener los extremos que se detallan en el Reglamento, entre ellos, quién es el responsable del fichero, la finalidad del fichero, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible, y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

Asimismo, deben comunicarse a la AEPD los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

El fichero solo se inscribe en el Registro General de Protección de Datos si la notificación se ajusta a los requisitos exigibles. En caso contrario, la AEPD puede pedir que se completen los datos que falten o se proceda a su subsanación.

Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la AEPD haya resuelto sobre la misma, se entiende inscrito el fichero a todos los efectos. Opera, pues, para la inscripción el silencio administrativo positivo.

C. Comunicación de la cesión de datos (art. 27).

Regla general: El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, debe informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

Excepciones:

a) Que la cesión venga impuesta por ley;

b) que el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros y para la finalidad que la justifique;

c) que la cesión deba efectuarse a las instituciones del Defensor del Pueblo, Ministerio Fiscal, jueces o tribunales, Tribunal de Cuentas, en ejercicio de sus funciones, o instituciones autonómicas equivalentes al Defensor del Pueblo o al Tribunal de Cuentas;

d) que la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos;

e) que la cesión se efectúe previo el procedimiento de disociación.

D. Datos incluidos en las fuentes de acceso público (art. 28).

Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales, deben limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado.

La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requiere el consentimiento del interesado, que podrá ser revocado en cualquier momento.

Los interesados tienen derecho a:

a) Que la entidad responsable del mantenimiento de los listados de los colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

b) Exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia debe realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, pierden el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, esta pierde el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se rigen por su normativa específica.

E. Prestación de servicios de información sobre solvencia patrimonial y crédito: las listas de morosos (art. 29).

Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito solo pueden tratar datos de carácter personal: a) obtenidos de los registros y las fuentes accesibles al público establecidos al efecto, o b) proce-

dentes de informaciones facilitadas por el interesado o con su consentimiento.

Pueden tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos, ha de notificarse a los interesados en el plazo de treinta días desde que se registren sus datos en el fichero, una referencia de los datos que se hayan incluido e informárseles de su derecho a recabar información de la totalidad de ellos. La notificación ha de hacerse por cada deuda concreta y determinada con independencia de que esta se tenga con el mismo o con distintos acreedores.

Cuando el interesado lo solicite, el responsable del tratamiento tiene el deber de comunicarle los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

Sólo se pueden registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos. El pago o cumplimiento de la deuda determina el deber de cancelación inmediata de todo lo relativo a la misma. En los restantes supuestos, los datos deben cancelarse a los seis años del vencimiento de la obligación.

El artículo 38 del Reglamento de la LOPD establece los requisitos para la inclusión de los datos en ficheros que sean deter-

minatnes para enjuiciar la solvencia económica del afectado: a) existencia previa de una deuda cierta, vencida, exigible y que haya resultado impagada; b) que no hayan transcurrido seis años desde la fecha en que hubo que proceder al pago de la deuda o del vencimiento de la obligación o del plazo concreto asi aquélla fuera de vencimiento periódico; y c) requerimiento previo de pago a quien corresponda el cumplimiento de la obligación[29].

F. Tratamientos con fines de publicidad y de prospección comercial (art. 30).

Quienes se dedican a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, solo pueden utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

Cuando los datos procedan de fuentes accesibles al público, en cada comunicación que se dirija al interesado se ha de informar del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

En el ejercicio del derecho de acceso, los interesados tienen derecho a conocer el origen de sus datos de carácter personal, así como del resto de información.

29. Véanse al respecto las sentencias del Tribunal Supremo de 15 de julio de 2010 y de 8 de febrero de 2012.

Los interesados tienen derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernen, en cuyo caso deben darse los datos de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

G. Censo promocional (art. 31).

Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de dirección, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, pueden solicitar del Instituto Nacional de Estadística (INE) o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

El uso de cada lista de censo promocional tiene un plazo de vigencia de un año. Transcurrido el plazo citado, la lista pierde su carácter de fuente de acceso público.

Los interesados pueden solicitar no aparecer en el censo promocional conforme a lo dispuesto en el Reglamento de la LOPD. El procedimiento es gratuito para los interesados y se incluye en el documento de empadronamiento. Trimestralmente se ha de editar una lista actualizada del censo promocional, excluyendo los nombres y domicilio de los que así lo hayan solicitado.

Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

El Reglamento de la LOPD desarrolla los procedimientos de formación del censo promocional, de oposición a aparecer en

el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establece, además, los plazos para la puesta en operación del censo promocional.

H. Códigos tipo (art. 32).

Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupan, pueden formular los llamados códigos tipo. Estos establecen las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas.

Los códigos tipo pueden contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establezcan deben respetar los principios fijados en aquél.

Los códigos tipo tienen el carácter de códigos deontológicos o de buena práctica profesional. Han de ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas.

El Registro General de Protección de Datos puede denegar la inscripción del código tipo cuando considere que no se

ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la AEPD requerir a los solicitantes para que efectúen las correcciones oportunas.

I. Entidades aseguradoras.

Las entidades aseguradoras pueden establecer ficheros comunes con datos de carácter personal para la liquidación de siniestros y la colaboración estadístico-actuarial, y así permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora.

La cesión de datos a estos ficheros no requiere el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable, para que se puedan ejercitar ante él los derechos de acceso, rectificación y cancelación.

También pueden establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, es necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quien sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud solo pueden ser objeto de tratamiento con el consentimiento expreso del afectado.

9. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD).

A. Naturaleza y régimen jurídico.

Como se ha dicho, el Tratado de Funcionamiento de la Unión Europea, en su artículo 16, y la Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 8, requieren que en cada Estado exista una autoridad independiente que garantice el respeto de las normas sobre protección de datos de carácter personal. Aquí no se hace sino reiterar lo que venían exigiendo las normativas europeas.

El Tribunal de Justicia de la Unión Europea ha considerado la creación de estas autoridades de control en cada uno de los Estados miembros como un "elemento crucial de la protección de las personas en lo que respecta al tratamiento de datos personales" (sentencia de 9 de marzo de 2010).

En España, la autoridad independiente que garantiza la normativa referida a la protección de datos es la Agencia Española de Protección de Datos (AEPD). El Tribunal Supremo, en su sentencia de 2 de diciembre de 2011, recoge las razones que justifican el nacimiento de la Agencia, su naturaleza y los fines que persigue esta en nuestro sistema jurídico en orden a la protección de datos de carácter personal.

La AEPD es un ente de derecho público (hoy con la categoría de "agencia estatal" conforme a la Ley 28/2006, de 18 de julio), con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones pú-

blicas en el ejercicio de sus funciones. Se rige por la LOPD y por su Estatuto propio, que se aprueba por el Gobierno.

En el ejercicio de sus funciones públicas, la AEPD actúa de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La AEPD ejerce sus funciones con total independencia y objetividad, y no está sujeta a instrucción alguna en el desempeño de aquéllas, ni sometida a la tutela de ningún órgano del Estado[30]. Esta independencia es válida tanto para el sector público como para el sector privado a cualquier escala territorial (estatal, autonómica, provincial, comarcal o municipal).

El proyecto de Reglamento General de Protección de Datos refuerza aún más las funciones, la independencia de la Agencia y de las autoridades de control que se creen y sus poderes (de intervención, investigación, órdenes imperativas, autorización, consulta, amonestación, advertencia, rectificación, prohibición, suspensión, sanción, ejercicio de acciones jurisdiccionales, emisión de dictámenes, e informe de su actividad).

B. Funciones.

Son funciones que tiene atribuidas la AEPD:

30. La sentencia de 9 de marzo de 2010, del Tribunal de justicia de la Unión Europea interpreta qué debe entenderse por "total independencia": la facultad de decisión exenta de toda influencia externa, ya sea directa o indirecta; y recuerda que "la garantía de la independencia no se ha establecido para conceder un estatuto particular a esas autoridades mismas o sus agentes, sino para reforzar la protección de las personas y de los organismos afectados por sus decisiones".

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Se trata de una función amplia, que convierte a la Agencia en una valedora y garante de esta legislación especial, con una extensa relación de potestades. Así, como reconoce la STS de 17 de noviembre de 2009, "la Agencia Española de Protección de Datos, como organismo que tiene encomendada la aplicación en vía administrativa de la legislación de protección de datos, puede y debe comprobar las circunstancias determinantes de la caracterización que a los hechos del caso legalmente corresponde".

Un ejemplo concreto de esta amplia función garantista puede verse en esta misma sentencia, que afirma que la Agencia puede incluso "examinar los contratos aportados para justificar que es aplicable el art. 12 LOPD. Si la Agencia razonablemente concluye que un contrato no reúne las condiciones exigidas por dicho precepto legal o sencillamente que no merece credibilidad, puede y debe concluir que ese contrato no es idóneo para justificar que el art. 12 LOPD es aplicable al caso. La Agencia ha de verificar todas las circunstancias relevantes para la aplicación de la legislación sectorial que tiene encomendada, incluidas aquéllas consistentes en actos y negocios privados. Esto no significa, naturalmente, que la Agencia pueda declarar la invalidez o la ineficacia de los contratos, ni hacer interpretaciones de los mismos vinculantes para las partes: en el plano civil, los contratos surtirán los efec-

tos que correspondan; pero la determinación de su relevancia para la aplicación de la legislación de protección de datos compete a la Agencia".

b) Emitir las autorizaciones previstas en la LOPD o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la LOPD.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas. El art. 18 de la LOPD esteblece una vía de tutela de los derechos de las personas afectadas a través de la presentación de una reclamación ante la AEPA. A ella se ha hecho referencia en la letra H) del número 5 precedente.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de estos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora prevista en la LOPD.

Ante posibles infracciones tipificadas en la LOPD, la Agencia tiene el deber jurídico de actuar en los términos previstos en esta Ley y, en consecuencia, tiene la obligación de abrir el procedimiento sancionador que corresponda. “Su inactividad, acordando el archivo de una denuncia, no está justificada y es contraria al ordenamiento jurídico y lesiva del derecho fundamental a la protección de datos de carácter personal" (STS de 16 de diciembre de 2010)”.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la LOPD.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estimen necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto ha de publicar periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

l) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la

recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.

m) Ejercer la potestad de control sobre los ficheros de las Administraciones públicas.

Las resoluciones de la AEPD se han de hacer públicas, una vez han sido notificadas a los interesados. La publicación se realiza preferentemente a través de medios informáticos o telemáticos.

C. El Registro General de Protección de Datos (art. 39).

El Registro General de Protección de Datos es un órgano integrado en la AEPD.

En él han de inscribirse:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la LOPD.

d) Los códigos tipo.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

En el Reglamento de la LOPD se regula el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes, y demás extremos pertinentes.

D. La potestad de inspección.

Las autoridades de control están legalmente habilitadas para inspeccionar los ficheros y recabar cuantas informaciones precisen para el cumplimiento de sus cometidos de vigilancia.

A tal efecto, pueden solicitar la exhibición o el envío de documentos y datos, y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

10. ENTIDADES DE LAS COMUNIDADES AUTÓNOMAS EQUIVALENTES A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Las Comunidades Autónomas pueden crear también entidades equivalentes a la Agencia Española de Protección de Datos en relación con ficheros de titularidad pública creados o gestionados por ellas o por la Administración Local de su ámbito territorial.

Estas entidades se consideran autoridades de control, y a ellas se les garantiza la misma plena independencia y objetividad en el ejercicio de su cometido que a la AEDP.

También pueden las Comunidades Autónomas crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

El Director de la AEDP puede convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la AEDP y los órganos correspondientes de las Comunidades Autónomas pueden solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Han creado su respectiva Agencia: a) la Comunidad de Madrid, mediante la Ley 13/1995, de 21 de abril, hoy derogada y sustituida por la Ley 8/2001, de 13 de julio, de protección de datos de carácter personal; b) Cataluña, mediante la Ley 5/2002, de 19 de abril, de la Autoridad Catalana de Protección de Datos Personales, derogada y sustituida por la Ley 32/2010, de 1 de octubre; y c) País Vasco, mediante la Ley 2/2004, de 25 de febrero, de la Agencia Vasca de Protección de Datos Personales.

Estatutos de Autonomía reformados recientemente, como el catalán (art. 31) o el de Castilla y León [art. 1.2 d)], prevén expresamente la existencia de una autoridad independiente, designada por el Parlamento, o la posible creación de una agencia autonómica, respectivamente.

En el caso de Navarra, la disposición adicional segunda de la Ley Foral 11/2007, de 4 de abril, para la implantación de la Administración de la Comunidad Foral de Navarra, faculta al Gobierno de Navarra a promover mediante Decreto Foral la crea-

ción de la Agencia de Protección de Datos Personales de Navarra, si bien esta no ha llegado a crearse, ni tampoco se ha anunciado siquiera su creación.

Todas estas autoridades autonómicas solo pueden ejercer sus competencias sobre ficheros de titularidad pública creados por las Administraciones de la Comunidad Autónoma o por las entidades locales, así como por organismos dependientes de ellas. En esto es clarificadora la STS de 19 de octubre de 2011, que concluye que una fundación hospitalaria creada por una Comunidad Autónoma (la fundación Hospital Alcorcón) es "una Institución creada por la Administración Pública, que actúa sometida a la tutela y control de la Administración Pública y financiada mediante ingresos públicos, por lo que se trata de una organización o entidad inequívocamente pública, que tras el traspaso de las funciones del protectorado, registro, tutela y control a la Comunidad de Madrid, tiene perfecto encaje entre las Administraciones de la Comunidad de Madrid a que se refiere el artículo 2 de la ley 8/2001, de Protección de Datos de Carácter Personal en la Comunidad de Madrid , cuyos ficheros por ellas creados o gestionados, están sujetos al control de la APDCM, con la única excepción de las empresas públicas con forma de sociedad mercantil".

Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

Cuando el Director de la AEPD constata que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de la LOPD en materia de su exclusiva competencia, puede requerir a la Administración

competente para que adopte las medidas correctoras que determine en el plazo que expresamente fije en el requerimiento.

Si la Administración pública no cumple el requerimiento formulado, el Director de la AEPD puede impugnar la resolución adoptada por esa Administración.

11. INFRACCIONES Y SANCIONES

A. Tipos de infracciones.

Las infracciones a la LOPD se califican en leves, graves o muy graves.

La relación de infracciones nos permite conocer lo que está prohibido en la gestión de los datos personales y, además, no da una perfecta idea de qué conductas son las más graves y, en consecuencia, suponen una vulneración más intensa del derecho fundamental de protección de datos personales.

1. Son infracciones leves:

a) No remitir a la AEPD las notificaciones previstas en la LOPD o en sus disposiciones de desarrollo.

b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en la LOPD.

2. *Son infracciones graves:*

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin la preceptiva disposición general, publicada en el BOE o en el diario oficial correspondiente.

b) Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto a la LOPD y sus disposiciones de desarrollo [art. 44.3 b) LOPD y STS de 12 de mayo de 2009].

c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD, salvo cuando el hecho sea constitutivo de infracción muy grave.

d) La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal [art. 44.3 d) LOPD y STS de 15 de junio de 2010. La STS de 21 de noviembre de 2011 no considera tratamiento el hecho de que un órgano de la Administración informe a otro órgano de otra Administración las denuncias y recursos contencioso-administrativos presentados por la recurrente].

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición (STS de 19 de mayo de 2010).

Como aclara la STS de 14 de mayo de de 2012, el incumplimiento por el responsable del fichero del plazo para contestar la solicitud de acceso puede tener consecuencias en un procedimiento sancionador, en base a las infracciones tipificadas en el artículo 44 de la LOPD, algunas de ellas relativas al impedimento y la obstaculación del ejercicio del derecho de acceso, lo que no sucedería en caso de tener dichas Resoluciones un contenido desestimatorio de la reclamación.

f) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la LOPD y sus disposiciones de desarrollo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal, sin las debidas condiciones de seguridad que reglamentariamente se determinan [art. 44.3 h) LOPD y SSTS de 20 de febrero y 13 de marzo de 2012].

i) No atender los requerimientos o apercibimientos de la AEPD o no proporcionarle cuantos documentos e informaciones solicite.

j) La obstrucción al ejercicio de la función inspectora.

k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en la LOPD y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave [art. 44.3 k) LOPD y SSTS de 23 de marzo de 2011 y de 23 de enero, 30 de enero y 14 de febrero de 2012).

3. Son infracciones muy graves:

a) La recogida de datos en forma engañosa o fraudulenta [art. 44.4 a) de la LOPD].

Esta infracción solo puede imponerse cuando los datos se han obtenido mediante el uso del engaño o fraude. No puede incluirse en este supuesto cualquier utilización de datos de forma irregular (STS de 27 de mayo de 2011). El Tribunal Supremo ha aclarado también que ambos términos, "engañoso" y "fraudulento" son sinónimos, por lo que hay que descartar que sean dos modalidades diferentes de comisión de la infracción. Por tal "engaño" se entiende la acción contraria a la verdad o a la rectitud, de la que resulta perjuicio para otro (SSTS de 5 de octubre de 2010, citada de 27 de mayo de 2011 y 27 de octubre de 2011).

En todo caso, para que pueda imponerse la sanción es necesario que haya quedado probado el engaño durante la tramitación del procedimiento sancionador (SSTS de 17

de marzo y de 29 de junio de 2010). Como afirma la STS de 22 de febrero de 2011, "si la Administración quiere sancionar determinada conducta como constitutiva de aquella infracción, deberá necesariamente acreditar en qué aspecto de dicha conducta radicó el fraude o la deslealtad. La tipicidad en materia sancionadora es una garantía elemental de civilización, antes incluso que del Estado de derecho en sentido propio; y, precisamente por ello, no cabe relajar su observancia so pretexto de lograr una mayor efectividad en la protección del bien jurídico tutelado por la norma sancionadora, que en este caso es el derecho a la vida privada. Así, si la prueba del fraude o la deslealtad es muy difícil por el carácter oculto de éstos, como dice el Abogado del Estado, la única conclusión aceptable con arreglo al principio de legalidad en materia sancionadora, consagrado por el art. 25 CE, es que el art. 44.4.) LOPD resultará escasamente aplicable en la práctica y que la Administración deberá esmerarse especialmente a la hora de hacer acopio del material probatorio de cargo. Esta Sala, en su reciente sentencia de 5 de octubre de 2010, ha tenido ocasión de afirmar que la aplicación del art. 44.4.a) LOPD exige ineludiblemente la prueba del fraude o la deslealtad, no sólo de la irregularidad en la recogida de datos".

b) Tratar o ceder los datos de carácter personal especialmente protegidos, salvo en los supuestos en que la LOPD lo autoriza, o violentar la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o la vida sexual.

El TS ha precisado recientemente que “tras la entrada en vigor de la reforma operada en la LOPD por (disposición final 56ª de) la ley 2/2011, de 4 de marzo, de Economía Sostenible), sólo está tipificado como infracción muy grave el tratamiento o cesión que afecte a los datos especialmente protegidos a que se refieren los apartados 2 , 3 y 5 del artículo 7 LOPD, que son los relativos a la ideología, afiliación sindical, religión y creencias, los que hagan referencia al origen racial, a la salud y a la vida sexual y los relativos a la comisión de infracciones penales o administrativas mientras que las demás cesiones que no tenga por objeto esta clase de datos se tipifican como falta grave en el artículo 44.3.k)LOPD , que se refiere a la comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en la LOPD y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave" (SSTS de 30 de enero, 5 de marzo, 7 de mayo y 27 de junio de 2012, entre otras).

c) No cesar en el tratamiento ilícito de datos de carácter personal cuando exista un previo requerimiento del Director de la AEPD para ello.

d) La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la AEPD, salvo en los supuestos en los que conforme a la LOPD y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

B. Tipo de sanciones.

1. Las infracciones leves se sancionan con multa de 900 a 40.000 euros.

2. Las infracciones graves se sancionan con multa de 40.001 a 300.000 euros.

3. Las infracciones muy graves se sancionan con multa de 300.001 a 600.000 euros.

La cuantía de las sanciones, dada la amplitud de su abanico y el excesivo campo que queda para que juegue el órgano sancionador, se gradúa atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción, la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

El órgano sancionador ha de establecer la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate (art. 45 LOPD y STS de 27 de junio de 2011, que recalca que es una manifestación específica del principio de proporcionalidad), en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en la LOPD [art. 45.5 a) de la LOPD y SSTS de 27 de junio de 2010, 3 de junio de 2011 y 5 de diciembre de 2011].

   Para el Tribunal Supremo, la propia redacción del art. 45.5 a) de la LOPD "remite, para su aplicación, a una valora-

ción de las circunstancias fácticas del caso en cuanto pongan de manifiesto esa disminución de la culpabilidad o de la antijuridicidad, con relevancia para moderar la cuantía de la sanción, en adecuada proporcionalidad a la entidad de los hechos sancionados. Como tales apreciaciones fácticas su fijación o determinación corresponde a la Sala de instancia lo que obliga a atenerse a la apreciación de la prueba hecha por ésta, salvo que se alegue alguna de las causas que permiten el acceso a casación de la valoración de la prueba" (STS de 3 de junio de 2011). También aclara la misma sentencia que la aplicación del precepto es igual para un actuar doloso, que para uno negligente.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

Excepcionalmente, el órgano sancionador puede, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto

responsable a fin de que, en el plazo que le determine, acredite la adopción de las medidas correctoras que en cada caso resulten pertinentes, siempre que concurran los dos siguientes presupuestos:

a) Que los hechos sean constitutivos de infracción leve o grave conforme a lo dispuesto en la LOPD.

b) Que el infractor no haya sido sancionado o apercibido con anterioridad.

Si no se atiende el apercibimiento en el plazo que el órgano sancionador haya determinado, procede la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

En ningún caso puede imponerse una sanción más grave que la fijada en la LOPD para la clase de infracción en la que se integre la que se pretenda sancionar.

El Gobierno está facultado para actualizar periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

El procedimiento sancionador se establece en el Reglamento de la LOPD. Por lo que se refiere a las denuncias, interesa destacar que, como ha declarado el TS, el denunciante carece de la condición de interesado en el procedimiento sancionador que se pueda incoar a resultas de su denuncia. El denunciante no puede impugnar la resolución final, aunque sí el archivo de la denuncia por la Administración (STS de 6 de octubre de 2009). Ahora bien, como esta misma sentencia destaca si bien "el de-

nunciante de una infracción de la legislación de protección de datos carece de legitimación activa para impugnar la resolución de la Agencia en lo que concierne al resultado sancionador mismo (imposición de una sanción, cuantía de la misma, exculpación, etc.) (….) llegado el caso, puede tener legitimación activa con respecto a aspectos de la resolución distintos del específicamente sancionador siempre que, por supuesto, pueda mostrar algún genuino interés digno de tutela".

También la STS de 27 de septiembre de 2010 reconoce que "el denunciante no tiene derecho al castigo del denunciado desde el momento en que la imposición de una sanción no revierte en su beneficio o no le evita un perjuicio, según reiterada jurisprudencia de esta Sala [sentencias de 6 de octubre de 2009, 16 de diciembre de 2008 y las que en ellas se citan, entre otras]. Y, desde luego, aquí los recurrentes no han puesto de manifiesto qué ventaja obtendrían de una eventual sanción".

C. Infracciones de las Administraciones públicas.

Cuando las infracciones se cometen en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, la Agencia o el órgano equivalente ha de dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Propiamente no es una sanción propiamente, sino un requerimiento imperativo de medidas a adoptar.

No queda claro en las normas estatales si la Agencia tiene legitimación procesal para impugnar ante la jurisdicción contencioso-administrativa el incumplimiento de por las

Administraciones infractoras de los requerimientos que les formula. Sin embargo, no deberían ponerse trabas formales en este sentido a una eventual intervención procesal de la Agencia, pues esta tiene en el asunto un interés legítimo y directo que va más allá de la defensa general de la pura legalidad (persigue la defensa y eficacia de sus actos administrativos en el caso concreto, no la prevalencia de normas generales), cuya capacidad procesal viene exigida como requisito por la Directiva comunitaria (art. 28.3), y el futuro Reglamento General de Protección de Datos no deja duda alguna de esa capacidad procesal cuando le reconoce, con carácter general, el poder de ejercitar acciones jurisdiccionales (art. 53.3 del proyecto).

Esta resolución se notifica al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hay.

El órgano sancionador puede proponer también la iniciación de actuaciones disciplinarias, si así lo viera procedente. El procedimiento y las sanciones a aplicar son las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

Las Administraciones afectadas han de comunicarse al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

Esta potestad solo puede ser ejercida por la Agencia o autoridad equivalente frente a las "Administraciones públicas". No se consideran tales los órganos judiciales (STS de 2 de diciembre de 2011). Ni tampoco lo son, a los efectos de la LOPD, los colegios

profesionales u oficiales en relación con los datos de sus colegiados, pues aquí tales colegios no ejercen potestades administrativas ni funciones públicas (STS de 20 de mayo de 2011). Como aclara la STS 1 de marzo de 2011, "la regla general es que las corporaciones sectoriales de base privada son personas privadas y sólo excepcionalmente, cuando ejercen potestades administrativas, tienen la condición de Administración Pública. (…). A la vista de cuanto se ha expuesto, y dado que la actuación del colegio oficial que fue objeto de denuncia ante la AEPD consistió en dar publicidad a una sentencia (con mención del nombre de uno de sus colegiados), sólo cabe concluir que no actuó en condición de Administración Pública: hablar de una sentencia en una revista no es ciertamente un acto de ejercicio de una potestad administrativa. Y frente a ello resulta irrelevante que el litigio que dio lugar a esa sentencia versara o no sobre actuaciones administrativas de COPAC, pues el dato incontestable es que esta corporación no tenía un deber administrativo de dar publicidad -o de dejar de darla- a dicha sentencia".

El Director de la AEPD está obligado a comunicar al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

D. Prescripción.

Las infracciones muy graves prescriben a los tres años, las graves a los dos años y las leves al año.

El plazo de prescripción comienza a contarse desde el día en que la infracción se ha cometido. Interrumpe la prescripción la iniciación, con conocimiento del interesado, del procedimiento

sancionador (art. 47.3 LOPD y STS de 16 de marzo de 2010), reanudándose el plazo de prescripción si el expediente sancionador está paralizado durante más de seis meses por causas no imputables al presunto infractor. No interrumpe la prescripción la resolución de diversos procesos civiles que no atañen a la persecución de la infracción ni a la reiteración de la misma (STS de 8 de junio de 2010).

Las sanciones impuestas por faltas muy graves prescriben a los tres años; las impuestas por faltas graves, a los dos años; y las impuestas por faltas leves, al año.

El plazo de prescripción de las sanciones comienza a contarse desde el día siguiente a aquel en que adquiere firmeza la resolución por la que se impone la sanción.

La prescripción se interrumpe por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

E. Procedimiento sancionador.

El Reglamento establece el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones.

Las resoluciones de la AEPD o del órgano equivalente de la Comunidad Autónoma agotan la vía administrativa.

Los procedimientos sancionadores tramitados por la AEPD, en ejercicio de las potestades que a la misma le atribuyen las

Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, han de tener una duración máxima de seis meses.

F. La potestad de inmovilización de ficheros.

El órgano sancionador puede, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos en los supuestos constitutivos de infracción grave o muy grave, en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pueda suponer un grave menoscabo de los derechos fundamentales de los afectados y, en particular, de su derecho a la protección de datos de carácter personal.

Si el requerimiento es desatendido, el órgano sancionador puede, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

PARTE II

LA PROTECCIÓN DE LOS DATOS PERSONALES RELACIONADOS CON LA SALUD

Juan Luis Beltrán Aguirre
Asesor Jefe del Defensor del Pueblo de Navarra

1. DERECHOS FUNDAMENTALES AFECTADOS.

En el ámbito de la asistencia sanitaria son dos los derechos constitucionales afectados: el derecho fundamental a la intimidad personal regulado en el art. 18.1 CE, si bien el ámbito propio de este derecho es la intimidad corporal, y el derecho fundamental a la protección de datos derivado del art. 18.4 CE pues según doctrina del Tribunal Constitucional recogida principalmente en sus Sentencias 1993/254, de 20 de julio, y 2000/292, de 30 de noviembre, contempla como un derecho fundamental independiente y desvinculado del derecho a la intimidad personal y familiar, aquel que tiene todo ciudadano a disponer libremente de sus datos personales.

Según señala la STC 2000/292, de 30 de noviembre, ambos derechos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar. Pero la peculiaridad del derecho fundamental a la protección de datos radica en su distinta función, objetivo y contenido.

La función del derecho fundamental a la intimidad (artículo 18.1 CE) es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar. Protege la intimidad personal, de la que forma parte la intimidad corporal (STC 37/1989), que en nuestro ámbito se traduce, por ejemplo, en poder disponer de habitación individual, y la llamada intimidad territorial, que significa que no se conozca o se haga pública la estancia de una persona en un centro sanitario[1].

En cambio, el derecho fundamental a la protección de datos (artículo 18.4 CE) persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con

1 Los artículos 29 y 30 de la Ley Foral 17/2010, de 8 de noviembre, disponen lo siguiente:

Artículo 29. Derecho a la intimidad.

1. Toda persona tiene derecho a ser atendida en un medio que garantice su intimidad, con especial respeto a su cuerpo durante la realización de los exámenes de diagnóstico, consultas y tratamientos médicos o quirúrgicos, cuidados, actividades de higiene y demás actuaciones sanitarias.

2. Toda persona tiene derecho a limitar, en los términos establecidos por la normativa vigente, la grabación y difusión de imágenes mediante fotografías, videos u otros medios que permitan su identificación.

(…)

Artículo 30. Habitaciones individuales.

En los centros hospitalarios del sistema sanitario público de Navarra o concertados con éste, se garantizará la disponibilidad de habitaciones individuales cuando las especiales circunstancias del paciente lo precisen, conforme a lo que reglamentariamente se establezca. El ejercicio de este derecho no podrá suponer un menoscabo del derecho a la asistencia sanitaria de otros usuarios del sistema.

el propósito de impedir un tráfico ilícito y lesivo para su dignidad. Así, el objeto del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino la reserva de todos los datos de carácter personal, particularmente los informatizados.

2. MARCO NORMATIVO.

El artículo 8 LOPD dispone que las instituciones, los centros públicos y privados y los profesionales pueden tratar los datos de salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad. Y, en efecto, la legislación sanitaria, como veremos seguidamente, contiene normas específicas y prevé excepcionar el régimen de protección de los datos de salud del paciente, pudiéndose acceder a ellos, ser tratados o cedidos en diversos supuestos, de los que daré cuanta a lo largo de este trabajo.

Así pues, el régimen jurídico de la protección de los datos de salud se articula a través de diversos instrumentos que operan en los ámbitos competenciales correspondientes: la Unión Europea, el Estado y las Comunidades Autónomas. En el ámbito europeo destacan las Directivas 95/46/CE y el art. 8 de la Carta Europea de Derechos Fundamentales de 7 de diciembre de 2000. De la normativa nacional estatal y de la foral cabe señalar, además de los citados artículos de la Constitución, las si-

guientes normas: Ley 14/1986, General de Sanidad, Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales (artículo 22), Ley Orgánica 15/1999, de Protección de Datos Personales, y su reglamento de desarrollo, Ley 34/2002, de Servicios de la Información y Comercio Electrónico, Ley 41/2002, básica reguladora de la Autonomía del Paciente, Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud, Ley 44/2003, de Ordenación de las Profesiones Sanitarias, Ley 59/2003, de Firma Electrónica, Ley 14/2006, de Técnicas de Reproducción Asistida Humana, Ley Orgánica 7/2006, de Protección de la Salud y Lucha contra el Dopaje en el Deporte, Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, Ley 14/2007, de Investigación Biomédica, Ley Foral 12/2009, de 19 de noviembre, de no discriminación por motivos de identidad de género y de reconocimiento de derechos de las personas transexuales, Ley Orgánica 2/2010, de 3 de marzo, de Interrupción Voluntaria del Embarazo, Real Decreto 1718/2010, de 17 de diciembre, de Receta Médica, Ley 33/2011, de 4 de octubre, General de Salud Pública (artículo 41), todas ellas con su normativa de desarrollo, además de las normas de calidad aplicables, como la ISO 17799:2005. A este arsenal legislativo debe añadirse, además de otras normas estatales no citadas, la legislación autonómica existente, cuya sola cita excedería las posibilidades de esta presentación.

No obstante, las normas esenciales para el estudio que nos ocupa son las siguientes:

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

- Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

- 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 (LBAP).

- Ley Foral 17/2010, de 8 de noviembre, sobre derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra.

En suma, la problemática de la confidencialidad y protección de los datos de salud tiene que ser abordada desde dos ámbitos normativos distintos, que se complementan y que, por ende, han de integrarse para una aplicación conjunta y armónica: de un lado, la LOPD, que tiene el carácter de ley general para el tratamiento de datos personales, a la que ha de acompañarse su Reglamento de 2007, y, de otro, la LBAP y, en su caso, legislación autonómica, que es la ley especial en materia de protección y tratamiento de datos de salud.

Y la armonización de estos dos bloques normativos no siempre es fácil, pues respecto de algunos supuestos, que estudiaremos más adelante, los regímenes jurídicos que establecen ambos bloques normativos son distintos, incluso antagónicos. Ello es debido, en primer lugar, al relevante papel que en la protección de datos de salud tiene la legislación sanitaria, ya que el artículo 8 de la LOPD remite directamente a la legislación estatal o autonómica sobre sanidad en lo que hace al tratamiento de datos de salud, y,

en segundo lugar, porque el bloque normativo relativo a la materia sanidad está integrado por profusa legislación autonómica que lo ha colmado, pero, a veces, con soluciones o respuestas distintas en razón de la opción elegida por cada legislador autonómico.

3. CONCEPTO DE DATOS PERSONALES DE SALUD Y DOCUMENTOS QUE LOS CONTIENEN.

1. Concepto de datos personales relacionados con la salud.

Según el artículo 5. 1. g) del Reglamento de la LOPD, los datos de carácter personal relacionados con la salud son "*las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética*". Y el artículo 7.1 de la LBAP establece que *toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley*.

El artículo 3 de la LBAP incorpora el concepto de información clínica, referido a "*todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla*".

El dato genético viene definido en el art. 3. j) de la Ley 14/2007, de Investigación Biomédica, como la "*información*

sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos"[2].

Conforme a la normativa expuesta, no siempre es fácil determinar, a priori, si estamos o no ante un dato de salud. Algunas veces, habrá de estarse al contexto en el que se maneja el dato. A título de ejemplo, la Agencia Española de Protección de Datos entiende que los datos relativos a las fechas de baja o alta de los trabajadores, asociadas a un código que permita la

2 En los biobancos se almacenan muestras biológicas que son una parte del cuerpo humano con información genética de una persona concreta. Es un soporte de datos genéticos distinto de los datos de salud, que se mantienen incluso después de la muerte, que podrían tener efectos para la familia biológica (incluida la descendencia). Obviamente, también están sometidos al régimen de protección de datos de salud.

GÓMEZ SÁNCHEZ, Y., en "La protección de los datos genéticos: el derecho a la autodeterminación informativa." Revista Derecho y Salud, núm. extraordinario, 2008, p. 61, destaca la singularidad de la información genética obtenida mediante análisis de ADN de cualquier tipo y naturaleza. En general:

-Permite al propio sujeto obtener información sobre su configuración genética, las consecuencias presentes o futuras de tal configuración, y le posibilita la adopción de decisiones y el ejercicio de sus derechos y libertades.

- Permite identificar al sujeto, vivo o muerto, y/o relacionarle con otros sujetos vivos o muertos.

- Permite conocer al sujeto -pero también a terceros- el estado de salud actual y prever la mayor o menor propensión a padecer patologías futuras.

- Permite detectar predisposiciones genéticas de los individuos (no necesariamente de carácter patológico) y capacidades de diversa naturaleza.

- Aporta datos relevantes que pueden trascender el ámbito exclusivamente individual para afectar a la descendencia, a un grupo familiar o étnico determinado y, en última instancia, a un "patrimonio genético" común -pero diverso- de toda la Humanidad.

- Puede aportar información para el futuro aunque la relevancia de dicha información no se conozca en el momento de extraer las muestras biológicas;

- Aporta datos que podrían ser utilizados en campos muy diversos de la organización de las sociedades (cultura, medio ambiente, educación, biodiversidad...).

identificación de la causa de la baja como motivada por enfermedad común, profesional o maternidad, es un dato de salud, pero que, sin embargo, no es un dato de salud cuando figuran únicamente las fechas y la indicación de "baja" u otros supuestos análogos de los que no pueda fácilmente deducirse que la baja se debe a algún tipo de enfermedad. La STS de 5 de marzo de 2012 –RJ/2012/4361–, también entiende que el sólo dato de la fecha de baja, sin ningún otro añadido o explicación no puede considerarse como un dato de salud. Respecto al dato de fumador o no fumador entiende la Agencia que si el dato no sirve para realizar evaluaciones de salud o médicas (por ejemplo, si lo es solo a efectos de expedir un billete de avión), no parece que sea un dato de salud, ya que, aunque sea un dato de riesgo potencial para la salud, no informa por sí solo del estado de salud pasado, presente o futuro de la persona. En caso contrario, sí será un dato de salud.

2. Documentos que los contienen.

El artículo 3 de la LBAP incorpora el concepto de documentación clínica, entendida como "*el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial*". Aparte de los informes clínicos que normalmente reciben todos los pacientes al finalizar el proceso asistencial (consulta externa, alta, urgencias, etcétera), interesa aquí enumerar en concreto los siguientes:

A. Historia Clínica.

Con carácter general el art. 3 de la LBAP, define la historia clínica como "*el conjunto de documentos que contiene los*

datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial". A su vez, el artículo 15.1 completa la regulación de la historia clínica disponiendo que "*todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada*". Por tanto, implícitamente establece el deber de elaborar la historia clínica de cada paciente.

Por su parte, el artículo 58.1 de la Ley Foral 17/2010, de 8 de noviembre, establece que la historia clínica recoge el conjunto de documentos relativos al proceso asistencial de cada enfermo, identificando a los médicos y demás profesionales asistenciales que han intervenido en el mismo. Añade que debe procurarse la máxima integración posible de la documentación clínica de cada paciente, y que dicha integración debe hacerse, como mínimo, en el ámbito de cada centro, donde debe existir una historia clínica única para cada paciente.

La historia clínica, por tanto, puede contener también fotografías del cuerpo o de partes del cuerpo del paciente, que quedan sometidas al mismo régimen de protección que el resto de datos clínico-asistenciales.

Su finalidad principal según el art. 15.2 de la LBAP es la de "*..facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud*".

Así pues, la legalmente necesaria elaboración de la historia clínica persigue que se garantice al ciudadano la mejor asistencia sanitaria posible, lo que, además, debe conseguirse respetando los derechos fundamentales a la intimidad y a la protección de los datos. Por tanto, la historia clínica no tiene como norte la salvaguarda de los derechos fundamentales del artículo 18 CE y, a partir de ahí, garantizar la asistencia sanitaria, sino justamente lo contrario[3]. Evidentemente, su elaboración y utilización exige la satisfacción íntegra de los derechos afectados, pero en caso de conflicto, no sólo de naturaleza jurídica, sino de otra índole, tales como organizativos, económicos o informáticos, cuando resulte forzado optar por la prevalencia de alguno de aquellos, entiendo que prima sobre los derechos fundamentales a la intimidad y a la protección de datos, el derecho a la asistencia sanitaria. Ello porque, en última instancia, así se preserva el derecho fundamental a la vida, que es presupuesto del ejercicio del resto de derechos.

Las historias clínicas de los servicios públicos están informatizadas o en proceso de informatización. De ahí que convenga recordar que el Anexo de la Ley 11/2007, de Acceso Electrónico a Servicios Públicos, define el documento electrónico como "*la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*".

Puede afirmarse que la historia clínica es el documento clínico más importante por ser el que contiene mayor número de datos del paciente. La LBAP enumera los datos mínimos que debe con-

3 Señala el artículo 60.1 de la Ley Foral 17/2010, de 8 de noviembre, que la historia clínica es un instrumento destinado fundamentalmente a ayudar a garantizar una asistencia adecuada al paciente.

tener la historia clínica, y cada norma autonómica hace lo mismo. Para Navarra, el contenido mínimo de la historia clínica viene fijado por el artículo 59 de la Ley Foral 17/2010, de 8 de noviembre. No obstante, interesa señalar que conforme al Real Decreto 1093/2010, de 3 de septiembre que aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, la historia clínica resumida debe contener, como mínimo, los datos establecidos en su Anexo VIII. Este Real Decreto, atendidas la diversidad de sistemas y tipos de historias clínicas vigentes en el ámbito de cada Comunidad Autónoma, establece el conjunto mínimo de datos que deben contener una serie de documentos clínicos con el fin de compatibilizar y hacer posible su uso por todos los centros y dispositivos asistenciales que integran el Sistema Nacional de Salud. Los documentos clínicos para los que se fija un conjunto mínimo de datos son los siguientes: a) informe clínico de alta (anexo I); b) informe clínico de consulta externa (anexo II); c) informe clínico de urgencias (anexo III); d) informe clínico de atención primaria (anexo IV); e) informe de resultados de pruebas de laboratorio (anexo V); f) informe de resultados de pruebas de imagen (anexo VI); g) informe de cuidados de enfermería (anexo VII); h) historia clínica resumida (anexo VIII).

En el ámbito de los Servicios Sociales, la historia social es el equivalente a la historia clínica en los centros sanitarios.

B. Receta médica.

La receta médica es el documento de carácter sanitario, normalizado y obligatorio, mediante el cual los médicos, odontólogos o podólogos, legalmente facultados para ello, y en el ámbito de sus competencias respectivas, prescriben a los pa-

cientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos. Puede ser expedida en papel o en formato electrónico.

La información que debe contener la receta médica viene descrita en el artículo 3 del Real Decreto 1718/2010, de 17 de diciembre, de receta médica. Las medidas de protección de la confidencialidad de los datos se establecen en los artículos 11 y 19 del referido Real Decreto.

La orden de dispensación hospitalaria para pacientes no ingresados es el documento de carácter sanitario, normalizado y obligatorio para la prescripción por los médicos, odontólogos y podólogos de los servicios hospitalarios, de los medicamentos que exijan una particular vigilancia, supervisión y control, que deban ser dispensados por los servicios de farmacia hospitalaria a dichos pacientes.

C. Documento de voluntades anticipadas.

Conforme al artículo 54 de la Ley Foral 17/2010, de 8 de noviembre, el documento de voluntades anticipadas es el dirigido al médico responsable en el cual una persona mayor de edad, o un menor al que se le reconoce capacidad conforme a la Ley Foral, deja constancia de los deseos previamente ex-

presados sobre las actuaciones médicas para cuando se encuentre en una situación en que las circunstancias que concurran no le permitan expresar personalmente su voluntad, por medio del consentimiento informado, y que deben ser tenidos en cuenta por el médico responsable y por el equipo médico que le asista en tal situación. En las voluntades anticipadas pueden incorporarse manifestaciones para que, en el supuesto de situaciones críticas, vitales e irreversibles respecto a la vida, se evite el sufrimiento con medidas paliativas aunque se acorte el proceso vital, no se prolongue la vida artificialmente por medio de tecnologías y tratamientos desproporcionados o extraordinarios, ni se atrase abusiva e irracionalmente el proceso de la muerte.

Se trata, por tanto, de un documento que se deposita en el hospital que contiene datos personales y manifestaciones relativas a la salud y asistencia sanitaria que se desea. Existe un Registro de Voluntades Anticipadas de Navarra[4], que a afectos de la LOPD se constituye en fichero. En dicho registro se inscriben los documentos de voluntades anticipadas, su modificación, sustitución y revocación, independientemente del procedimiento de formalización empleado, con objeto de garantizar su conocimiento por los facultativos de los centros asistenciales, tanto públicos como privados.

Se ha de garantizar la confidencialidad y seguridad de los datos contenidos en el documento de voluntades anticipadas conforme a la LOPD. Las personas que accedan a los datos del Registro de Voluntades Anticipadas están obligadas a guardar secreto.

4 Creado por Decreto Foral 140/2003, de 16 de junio.

D. Tarjeta sanitaria individual.

El artículo 2 del Real Decreto 183/2004, de 30 de enero, por el que se regula la Tarjeta Sanitaria Individual, establece que las Administraciones sanitarias autonómicas y el Instituto Nacional de Gestión Sanitaria emitirán una tarjeta sanitaria individual con soporte informático a las personas residentes en su ámbito territorial que tengan acreditado el derecho a la asistencia sanitaria pública. Esta tarjeta será válida en todo el Sistema Nacional de Salud, y permitirá el acceso a los centros y servicios sanitarios del sistema en los términos previstos por la legislación vigente.

A su vez, el nuevo artículo 3 bis de la Ley 16/2003, de 28 de mayo de cohesión y calidad del SNS, dispone que la tarjeta sanitaria individual (TSI) es un documento personalizado que permite identificar al usuario del Sistema Nacional de Salud de forma unívoca, y que acredita el derecho a la asistencia sanitaria pública[5].

Es un soporte físico, en forma de tarjeta, en cuyo anverso se estampa, en relieve, en la línea superior los códigos de identificación de tipo de tarjeta e identificación personal de acuerdo con las normas de referencia; en la segunda línea se fija el tipo de usuario y

5 También existe la Tarjeta Sanitaria Europea (TSE) como el documento personal e intransferible que acredita el derecho de su titular a recibir las prestaciones sanitarias que resulten necesarias, desde un punto de vista médico, durante su estancia temporal por motivos de trabajo, estudios, turismo, en el territorio de la Unión Europea (Alemania, Austria, Bélgica, República Checa, Chipre, Dinamarca, Eslovaquia, Eslovenia, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, Suecia, Bulgaria y Rumanía), del Espacio Económico Europeo (Islandia, Liechtenstein, Noruega) y en Suiza, teniendo en cuenta la naturaleza de las prestaciones y la duración de la estancia, de acuerdo con la legislación del país de estancia. La Tarjeta Sanitaria Europea no es válida cuando el desplazamiento tiene la finalidad de recibir un tratamiento médico.

su número de afiliación al sistema; en la tercera, el número del DNI en todos aquellos usuarios que dispongan de él, y por último, en la cuarta línea aparece impreso el nombre y apellidos del usuario. La banda magnética de tres pistas, situada en el reverso de la tarjeta, contiene actualmente la información numérica y alfanumérica correspondiente a los códigos de identificación del tipo de tarjeta, clase de usuario, apellidos y nombre, y fecha de caducidad. Incorporará también la clasificación establecida mediante código alfanumérico de su nivel de renta.

Se pretende también la interoperabilidad de la TSI unificando sus contenidos e incorporando la historia clínica digital, que tiene el objetivo de garantizar la disponibilidad de la información clínica básica de los pacientes cuando requieran de asistencia sanitaria independientemente de la Comunidad Autónoma en la que se encuentren. Véase el Real Decreto 1093/2010, de 3 de septiembre.

4. EL TRATAMIENTO DE DATOS RELACIONADOS CON LA SALUD.

1. Nivel de protección: especial protección.

No cabe duda de que los datos de salud se sitúan en la esfera más íntima de la persona, particularmente, aquellos datos que su conocimiento por otros puede menoscabar el desarrollo de la personalidad, como lo son la orientación sexual, el padecimiento de enfermedades psiquiátricas o de transmisión sexual, embarazos interrumpidos, fertilidad, ser alcohólico o exalcóholico, etc. Su tratamiento inadecuado puede vulnerar otros derechos fundamentales, particularmente, a la no discriminación. De ahí que el artículo 7 de la LOPD califica los datos

de salud como especialmente protegidos y, al respecto, precisa en su apartado 3 que los datos de carácter personal que hagan referencia a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. Así pues, los datos de salud disfrutan de un estatuto jurídico particular dada su calificación de datos especialmente protegidos.

2. Principios informantes de la recogida y tratamiento de datos de salud.

La LOPD sienta unos principios que, sucintamente comentados, son los siguientes:

- Proporcionalidad, de manera que solo pueden ser recogidos y tratados los datos que sean adecuados, pertinentes y no excesivos con las finalidades explícitas y legítimas para las que se hayan obtenido.

- Limitación de objetivos, que en el ámbito sanitario no es otro que el de facilitar la asistencia sanitaria, si bien se contemplan algunas excepciones, como veremos.

- Exactitud de los datos, hasta el punto de que la rectificación de datos inexactos ha de hacerse de oficio.

- Cancelación de datos innecesarios, principio que, sin embargo, tiene importantes brechas en el ámbito sanitario, como también veremos.

- Transparencia y autonomía de la voluntad, lo que afecta a la información en la recogida de los datos, consentimiento en relación tanto con el tratamiento de los datos de salud como el acceso a los mismos, y el derecho de oposición al tratamiento.

- Confidencialidad y seguridad en el tratamiento.

3. Obligaciones previas al tratamiento de los datos: creación, notificación e inscripción de ficheros de titularidad pública y privada.

Fichero es todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Por tanto, manuales e informatizados[6].

Deben declararse todos aquellos ficheros que contengan datos de carácter personal, tanto si son informatizados, manuales estructurados o parcialmente informatizados (mixtos), siempre que estén identificadas o sean identificables las personas titulares de los datos.

---

6 Son ejemplos de ficheros sanitarios:

- Archivo de Historias Clínicas. Finalidad y usos: datos de la historia clínica del paciente para su seguimiento, gestión de la actividad asistencial, prestación farmacéutica, facturación, actividad docente, de investigación sanitaria y estadísticas. Sistema de información y vigilancia de problemas de salud pública. Finalidad y usos: vigilancia de la salud pública y registro de datos de personas físicas para la vigilancia de los riesgos para la salud pública, promoción y prevención de la salud, investigación epidemiológica..

- Gestión asistencial. Finalidad y usos: gestión de la actividad asistencial, facturación, control de pacientes. ➢

No pueden crearse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición que los crea. La LOPD tipifica como infracción grave "*proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente*". También tipifica como infracción leve, cuando no sea constitutivo de infracción grave, "*no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos*".

El contenido mínimo de la disposición de creación del fichero viene descrito en el artículo 54 del Reglamento LOPD[7].

Actualmente, son muchos los centros sanitarios y de servicios sociales que prestan una actividad sanitaria y socio-sanitaria. La actividad sanitaria se desarrolla por profesionales sanitarios.

➢ - Registro de cuidados paliativos de SNS-O. Finalidad: registro e pacientes oncológicos en tratamiento paliativo.

- Sistema de información y vigilancia de problemas de salud pública. Finalidad y usos: vigilancia de la salud pública y registro de datos de personas físicas para la vigilancia de los riesgos para la salud pública, promoción y prevención de la salud, investigación epidemiológica.

- Gestión asistencial. Finalidad y usos: gestión de la actividad asistencial, facturación, control de pacientes.

- Registro de cuidados paliativos de SNS-O. Finalidad: registro e pacientes oncológicos en tratamiento paliativo.

7. "La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia. ➢

La asistencia social por trabajadores sociales. Entonces, se debe tener especial cuidado en diferenciar y separar el archivo y custodia de los datos de la historia social de aquellos que tienen como fin específicamente la asistencia sanitaria, que se integran en la historia clínica. La historia social sólo debe recoger aquellos datos de salud que repercutan en la situación personal y social del usuario de la prestación social. De ahí que es recomendable se separen y se traten separadamente en distintos ficheros la historia social y la historia clínica, y que se configuren perfiles de acceso para cada profesional que trabaje en Sanidad y en Servicios Sociales, de manera que sólo accedan a los datos necesarios para el ejercicio de sus funciones.

La complejidad que conlleva cada uno de los aspectos aludidos es enorme ya que se trata de un marco en el que el dato de salud merece una especial protección. Por ello, a los problemas generales que conlleva la aplicación de las medidas contempladas en la LOPD y su reglamento a cualquier fichero que contenga datos personales, se les añaden los particulares que se presentan cuando dichos datos personales son de salud.

➢ c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente Reglamento."

Cada vez es más frecuente la gestión indirecta por entidades privadas, mediante concesión, concierto, etc., de centros y servicios sanitarios. En estos casos, a las entidades privadas gestoras se les ha de aplicar el régimen de los ficheros privados, que tienen menos beneficios que los públicos (cesión de datos entre Administraciones Públicas sin consentimiento). En efecto, según el Reglamento de la LOPD, la utilización de una forma jurídica privada (sociedad mercantil) para gestionar el centro o servicio, requiere ficheros privados, y la utilización de una forma pública (ente público), exige la creación de ficheros públicos. Véase al respecto la STS de 19 de octubre de 2011 -RJ/2012/1295-.

Los ficheros de datos de titularidad privada deben ser notificados a la AEPD con carácter previo a su creación. La notificación debe incorporar similares datos a los públicos (artículo 55.2 del Reglamento de la LOPD).

4. La información y el consentimiento para el tratamiento de datos de salud.

A. La información debida.

En la primera fase del tratamiento de los datos, la autonomía personal se manifiesta en el derecho de los ciudadanos a conocer y determinar qué datos sobre su salud van a ser recogidos y registrados. Así, establece el artículo 5 LOPD que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos

y de los destinatarios de la información.

- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En el ámbito de la información que nos ocupa, es conveniente distinguir la información para el tratamiento de datos de salud de la información clínica para que el paciente pueda ejercer su derecho de autodeterminación a través del consentimiento informado. En la información que se debe dar para la recogida de los datos de salud del paciente, no tiene lógica ni sentido que cada vez que se hace un acto médico y se recaban nuevos datos, haya de practicarse nuevamente la información. Por el contrario, la información clínica ha de facilitarse cada vez que se hace un nuevo acto médico (artículo 4.2 LBAP).

Para dar cumplimiento al deber de información para el tratamiento de datos de salud pueden utilizarse diferentes medios. Uno de los que propone la LOPD es la inclusión de textos informativos en los impresos y cuestionarios que se utilicen en el momento de ingreso en el centro sanitario. De modo complementario pueden colocarse carteles informativos, accesibles

a los ciudadanos, en los puntos en que se realice la recogida de los datos. Para la recogida de los datos conviene analizar en cada supuesto concreto las peculiaridades del colectivo del que se están recogiendo (menores, mayores, discapacitados, etc.) y la forma más efectiva para que se dé cumplimiento al deber establecido legalmente. En cualquier caso, ha de llevarse a cabo a través de un medio que permita acreditar su cumplimiento (artículo 18 Reglamento LOPD) y corresponde al responsable del fichero la prueba del cumplimiento de la información.

B. El consentimiento expreso para el tratamiento de datos. Excepciones en el ámbito de datos de salud.

Cabe diferenciar aquí lo que es tratamiento de imágenes personales por el centro y lo que es tratamiento de los datos relativos a la salud de la persona, esto es, datos clínico-asistenciales, que también pueden contener imágenes (fotografías).

Respecto a la grabación y difusión de imágenes personales por los centros, dispone el artículo 32 de la Ley Foral 17/2010, de 8 de noviembre, que las personas usuarias de los centros, servicios y establecimientos sanitarios tienen derecho a que en ellos se limite, en los términos establecidos por la normativa estatal vigente, la grabación y difusión de imágenes mediante fotografías, vídeos u otros medios que permitan su identificación como destinatarios de atenciones sanitarias, debiendo obtenerse para tales actuaciones, una vez explicados claramente los motivos de su realización y el ámbito de difusión, la previa y expresa autorización de la persona afectada o de quien corresponda.

En cuanto a los datos clínico-asistenciales, el artículo 6 LOPD dispone que el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa[8]. A renglón seguido, y de manera específica para datos de salud, el artículo 7.3 LOPD establece que sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. A su vez, el artículo 31.1 de la Ley Foral 17/2010, de 8 de noviembre, establece que toda persona tiene derecho a la confidencialidad de toda la información relacionada con los datos referentes a su salud y estancias en centros sanitarios públicos o privados, y a que nadie que no cuente con su autorización pueda acceder a ellos, salvo cuando así lo autorice por razones de interés general la legislación vigente.

No obstante, el artículo 6.2 en relación con el 7.6 LOPD, establece unas excepciones en los siguientes términos: pueden ser objeto de tratamiento los datos de salud sin consentimiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto. Igualmente, conforme al párrafo segundo del citado artículo 7.6 también pueden ser objeto de tratamiento los datos cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra

8. Por ejemplo, Ley Orgánica de Protección de la Salud y de la Lucha contra el Dopaje en el Deporte; Ley sobre Tráfico y Circulación de Vehículos de Motor y Seguridad Vial; Ley de Prevención de Riesgos Laborales, Ley General de Salud Pública, etc.

persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. Subyace aquí la prevalencia del derecho a la vida sobre el derecho a la intimidad o la protección de datos personales (Según el TC sin vida no hay derecho a la intimidad: STC 1985/53). A lo dicho hay que añadir lo previsto en el artículo 8 LOPD que habilitan a las instituciones y centros sanitarios, tanto públicos como privados, y a los profesionales, a proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos de acuerdo con la legislación estatal o autonómica sobre sanidad.

Estas excepciones cubren solamente el tratamiento de datos con el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia, y a efectos de la gestión de estos servicios sanitarios, como, por ejemplo, facturación, contabilidad, estadísticas o planificación asistencial del servicio. No cubre el tratamiento posterior que no sea necesario para la prestación directa de tales servicios como la investigación médica, o el reembolso de gastos por un seguro de enfermedad. Tampoco cubre otras finalidades como controlar el absentismo laboral. La Audiencia Nacional, en Sentencia de 31 de mayo de 2002 señaló que la excepción prevista en el artículo 7.6 LOPD ha de ser interpretada restrictivamente, considerando que es preciso atender en cada caso concreto a que el tratamiento se dirija efectivamente a la prevención y el diagnóstico. En este sentido, un tratamiento para un fin distinto (en el caso analizado, el control del absentismo laboral) en que estas finalidades pueden ser consideradas "secundarias", a criterio del Tribunal no se encuentra amparado por lo dispuesto en la LOPD. En este mismo

sentido se pronunció también la Sentencia de la Audiencia Nacional de 23 de noviembre de 2006 –RJCA/2006/902-, respecto de la cual el Tribunal Supremo declaró no haber lugar al Recurso de casación para unificación de doctrina interpuesto contra la misma, en Sentencia de 12 de diciembre de 2007.

Así pues, en la relación ordinaria médico-paciente basta con el consentimiento previo que se deriva de la relación de los usuarios con los centros y profesionales sanitarios para admitir también el tratamiento de sus datos sin necesidad de que presten un consentimiento específico. Al respecto, es preciso tener presente que tanto la LBAP como la Ley Foral 17/2010, de 8 de noviembre, parten del contrato verbal y obligan imperativamente a establecer un contenido mínimo de los datos sanitarios en las historias clínicas, contenidos mínimos que necesariamente han de ser tratados[9]. En suma, el consentimiento para recibir asistencia conlleva el consentimiento para el tratamiento de los datos de salud.

Pero, además, existen supuestos en que la normativa expresamente escusa la necesidad de consentimiento expreso o implícito. Así, por ejemplo:

9. El artículo 59 de la Ley Foral 17/2010, de 8 de noviembre, establece el siguiente contenido de la historia clínica. 1. La historia clínica debe tener un número de identificación y debe incluir los siguientes datos: **a) Datos de identificación del enfermo y de la asistencia:** Nombre y apellidos del enfermo. Fecha de nacimiento. Sexo. Código de identificación personal contenido en la tarjeta sanitaria individual. Domicilio habitual y teléfono. Fecha de asistencia y de ingreso, si procede. Indicación de la procedencia, en caso de derivación desde otro centro asistencial. Servicio o unidad en que se presta la asistencia, si procede. Número de habitación y de cama, en caso de ingreso. Médico responsable del enfermo. **b) Datos clínico-asistenciales:** Antecedentes familiares y personales fisiológicos y patológicos. Descripción de la enfermedad o el problema de salud actual y motivos sucesivos de consulta. Procedimientos clínicos empleados y sus resultados, con los dictámenes correspondientes emitidos en caso de procedimientos o exámenes especializados, y también las hojas de interconsulta. Hojas de curso clínico, en caso de ingreso. Hojas de tratamiento médico. ➢

a) Conforme al artículo 19 del Real Decreto 1718/2010, de 17 de diciembre, de receta médica, no es necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, siempre que las citadas actuaciones tengan por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud, incluidos los distintos regímenes especiales de las Mutualidades de Funcionarios.

b) El artículo 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, exime del consentimiento el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población.

Frente al tratamiento de datos sin necesidad de previo consentimiento, la LOPD prevé el derecho de oposición, que se define como aquella facultad que tiene el interesado consistente en

➢ Hoja de consentimiento informado, si procede. Hoja de información facilitada al paciente en relación con el diagnóstico y el plan terapéutico prescrito, si procede. Informes de epicrisis o de alta, en su caso. Documento de alta voluntaria, en su caso. Informe de necropsia, si existe. En caso de intervención quirúrgica, debe incluirse la hoja operatoria y el informe de anestesia, y en caso de parto, los datos de registro. El informe de urgencia. La autorización de ingreso. El informe de anatomía patológica. En su caso, el documento de voluntades anticipadas, así como posible condición de donante de órganos. La evolución y planificación de los cuidados de enfermería. La aplicación terapéutica de enfermería. El gráfico de constantes. El informe clínico de alta. **c) Datos sociales:** Informe social, si procede.

oponerse a un determinado tratamiento de sus datos en aquellos supuestos en los cuales la normativa permite recogerlos sin su consentimiento. Para la Agencia Española de Protección de Datos es necesario que se den dos condiciones: a) que una Ley no prohíba expresamente ejercer la oposición; b) que exista un motivo fundado y legítimo para oponerse al tratamiento[10].

Aunque no se trata de datos de salud, sino de datos personales derivados del ejercicio por facultativos de la objeción de conciencia, una mención específica merece, en mi criterio, la cláusula existente en el modelo de declaración de objetor de conciencia contenida en la Ley Foral 16/2010, de 8 de noviembre, por la que se crea el Registro de objetores de conciencia, en cuanto el objetor consiente necesariamente la recogida y tratamiento de sus datos de carácter personal. Por algún sector se ha reputado de inconstitucional este obligado -no voluntario- consentimiento incorporado a la declaración formal que ha de hacer el facultativo. Pues bien, al respecto, cabe recordar, de entrada, que el artículo 7.2 de la LOPD únicamente permite el tratamiento de datos de carácter personal que revelen la ideología de una persona en el supuesto de que se haya manifestado previamente el consentimiento expreso y por escrito del interesado, precepto que trae causa del artículo 16.2 CE en cuanto dispone que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Sin embargo, el artículo 19.2 de la Ley Orgánica 2/2010, de 3 de marzo, exige una manifestación expresa efectuada por el interesado y firmada por el mismo, lo que implica una declaración pública que impide que la misma pueda quedar reservada a la esfera íntima de la persona. De ello resulta, como ha afirmado la Agen-

10. Memoria del año 2000 de la AEPD.

cia Española de Protección de Datos Personales[11], que dicha manifestación y el consentimiento para el tratamiento de los datos van irremisiblemente unidos, de manera que la propia manifestación haciendo pública la condición de objetor conlleva la prestación del consentimiento. Pues bien, este es el alcance y virtualidad de esa cláusula, que cumple, además, la función de informar al interesado del tratamiento de sus datos conforme exige el artículo 5 de la LOPD. No hay, pues, restricción desproporcionada del ejercicio del derecho de otorgar el consentimiento. En la cláusula no se ha hecho otra cosa que recoger las previsiones de la LOPD. Además, el tratamiento de los datos ha de limitarse, como es obvio, a los datos identificativos del profesional y a su condición de objetor, nada más. Las razones por las que se es objetor no han de declararse, quedando en el ámbito íntimo de la persona.

5. Medidas de seguridad en el tratamiento de datos de salud: aspectos generales.

A. Niveles de seguridad.

Con carácter general, los centros públicos sanitarios y de servicios sociales tienen que implantar las medidas de seguridad adecuadas al grado de protección que requieran los datos contenidos en cada uno de los ficheros, atendiendo a lo dispuesto en las normas de aplicación.

Tanto para los ficheros automatizados como para los manuales (ubicados en archivadores, armarios u otros soportes) o

11. Informe 272/2010.

parcialmente automatizados (mixtos), las medidas de seguridad se clasifican en tres niveles, básico, medio y alto, en función de la naturaleza de la información tratada. En el ámbito de los servicios sanitarios y sociales, con carácter general, los ficheros de datos de salud deben tener medidas de seguridad de nivel alto.

Respecto de las medidas de seguridad de nivel alto, además del Registro de accesos del que más tarde hablaré, el artículo 103 del Reglamento de la LOP exige que la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realice cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

No obstante, en lo que hace a concretos datos de salud precisa el artículo 81 del Reglamento LOPD lo siguiente:

> 5. *En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:*
>
> *a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.*
>
> *b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se*

contengan aquellos datos sin guardar relación con su finalidad.

6. *También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos*[12].

Además de las medidas de seguridad de nivel alto que se derivan de la LOPD, la legislación sectorial puede establecer medidas específicas o adicionales de seguridad. Al respecto, es destacable el artículo 21 de la Ley Orgánica 2/2010, de 3 de marzo, de Interrupción Voluntaria del Embarazo, que establece el siguiente régimen especial para el tratamiento de datos:

12. El alcance que la AEPD da a esta excepción en el informe jurídico emitido el 1 de julio de 2008, es el siguiente:"En consecuencia, de lo señalado en el presente informe cabe concluir que será de aplicación la previsión contenida en el artículo 81.6 del Reglamento de desarrollo de la Ley Orgánica y, en consecuencia, será únicamente exigibles las medidas de seguridad de nivel básico en aquellos ficheros que contengan uno o varios de los siguientes datos:

    - La mera indicación del grado de porcentaje de minusvalía del afectado o de los miembros de su unidad familiar a los efectos previstos para el cálculo de las retenciones en la legislación reguladora del Impuesto sobre la Renta de las Personas Físicas.
    - La indicación de datos "apto" o "no apto" de un trabajador a los efectos previstos en la Ley de Prevención de Riesgos Laborales.
    - Los datos relacionados con las obligaciones impuestas al empresario por la legislación vigente en materia de seguridad social que se limiten a señalar la existencia o no de enfermedad común, enfermedad profesional o accidente laboral o no laboral, así como la incapacidad laboral del trabajador.

- En el momento de la solicitud de información sobre la interrupción voluntaria del embarazo, los centros, sin proceder al tratamiento de dato alguno, han de informar a la solicitante que los datos identificativos de las pacientes a las que efectivamente se les realice la prestación son objeto de codificación y separados de los datos de carácter clínico asistencial relacionados con la interrupción voluntaria del embarazo.

- Los centros que presten la interrupción voluntaria del embarazo deben establecer mecanismos apropiados de automatización y codificación de los datos de identificación de las pacientes atendidas, considerándose datos identificativos de la paciente su nombre, apellidos, domicilio, número de teléfono, dirección de correo electrónico, documento nacional de identidad o documento identificativo equivalente, así como cualquier dato que revele su identidad física o genética.

- En el momento de la primera recogida de datos de la paciente, se le asigna un código que será utilizado para identificarla en todo el proceso.

- Los centros deben sustituir los datos identificativos de la paciente por el código asignado en cualquier información contenida en la historia clínica que guarde relación con la práctica de la interrupción voluntaria del embarazo, de forma que no pueda producirse con carácter general, el acceso a dicha información.

- Las informaciones relacionadas con la interrupción voluntaria del embarazo deben ser conservadas en la historia clínica de tal forma que su mera visualización no sea posible salvo por el personal que participe en la práctica de la prestación.

- No es posible el tratamiento de la información por el centro sanitario para actividades de publicidad o prospección comercial. No podrá recabarse el consentimiento de la paciente para el tratamiento de los datos para estas actividades.

B. Documento de seguridad.

El responsable del fichero o tratamiento, tanto sea informatizado como manual, debe elaborar un documento de seguridad que recoja las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, y que es de obligado cumplimiento para el personal con acceso a los sistemas de información.

El documento de seguridad puede ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También pueden elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, ha de tener el carácter de documento interno de la organización.

El documento debe contener, como mínimo, los aspectos reseñados en el artículo 88.3 del Reglamento de la LOPD.

C. El responsable del fichero y el encargado del tratamiento.

a) Centros públicos.

Conforme al artículo 3 de la LOPD el responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

En los ficheros de titularidad pública, el responsable del fichero es el órgano administrativo que tiene capacidad de decidir sobre el contenido, finalidad y uso del tratamiento de datos que se realiza. El responsable de un fichero debe indicarse expresamente en el correspondiente anexo de la disposición en la que se crea el mismo. En Navarra sería la Dirección del Complejo Hospitalario: artículo 61.5 de la Ley Foral 17/2010, de 8 de noviembre.

El Reglamento de desarrollo de la LOPD prevé la posibilidad de la existencia de varios responsables para un único fichero o tratamiento de datos de carácter personal (por ejemplo cuando en un centro sanitario se realicen diferentes actividades, siendo cada una de ellas competencia de diferentes órganos e instituciones sanitarias). En este caso, cada uno de los responsables debe notificar, a fin de proceder a su inscripción en el Registro de Ficheros de Datos Personales, la inscripción del correspondiente fichero.

Conforme al artículo 5 del Reglamento LOPD, el encargado del fichero es quien, en la práctica, trata físicamente los datos y los soportes, careciendo de autonomía y actuando siempre por cuenta y riesgo del responsable. Particularmente, controla el acceso al fichero. En los hospitales, la gestión de un fichero de historias clínicas

corresponde a las Unidades de Admisión y Documentación Clínica (artículo 61.5 de la Ley Foral 17/2010, de 8 de noviembre).

b) Centros privados concertados.

No parece que una entidad privada que preste un servicio público en el marco de un contrato de gestión de servicios públicos, pueda ser considerado un simple encargado del tratamiento. Se trata de cesiones de datos en las que el centro contratado tiene el carácter de responsable del fichero, que es privado, al llevar a cabo una actividad asistencial y conservar con esa finalidad la historia clínica[13]. El artículo 14.2 de la LBAP atribuye la responsabilidad del fichero a cada centro sanitario y al profesional individual, que deben conservar las historias clínicas de sus pacientes. El paso de un modelo de historia clínica descentralizada en cada uno de los centros a un modelo de historia clínica centralizada e informatizada a nivel de Servicio Autonómico de Salud transforma estas cesiones de historias clínicas en accesos dentro del marco del mismo responsable del fichero.

D. Prohibición de acceso sin autorización o habilitación legal y deber de secreto.

a) Prohibición de acceso.

Recordemos que el artículo 7.1 de la LBAP establece que nadie puede acceder a datos de salud sin previa autorización amparada por la Ley.

13. En este mismo sentido se pronuncia el informe 0501/2005 de la Agencia Española de Protección de Datos.

Conforme a la Recomendación 2/2004 de la Agencia de Protección de Datos de la Comunidad de Madrid, en la Unidad de Admisión y Documentación Clínica debe constar una relación detallada de todo el personal con posibilidad de acceso a las historias clínicas. Dicha relación debe hacerse de forma nominativa y por perfiles profesionales, diferenciando entre el personal profesional sanitario y el personal administrativo, y definiendo qué documentos son accesibles a ambos tipos de personal. A estos efectos, recomienda que toda la documentación clínica que forma parte del contenido de la historia clínica se archive separadamente de toda la documentación administrativa.

El artículo 197.2 del Código Penal tipifica como delito el que, sin estar autorizado, en perjuicio de tercero, acceda a datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

b) Deber de secreto.

El derecho a que se mantenga la confidencialidad de los datos de salud tiene como reverso el deber de secreto de quien accede a los mismos para el desempeño de sus funciones. A partir de la LBAP se ha producido una ampliación de los sujetos tradicionalmente obligados al secreto profesional, en cuanto su artículo 16.6 hace recaer esta obligación sobre cualquier persona que tenga acceso a la información contenida en las historias clínicas.

Por su parte, el artículo 10 de la LOPD establece que el responsable del fichero y quienes intervengan en cualquier fase del tra-

tamiento de los datos están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsisten aún después de finalizar sus relaciones con el titular del fichero, o, en su caso, con el responsable del mismo.

El art. 199.2 del Código Penal tipifica como delito la revelación de secretos profesionales[14]. Según expresa la STS de 4 de abril de 2001 –RJ/2001/2016-, para el ámbito sanitario con ocasión de la revelación a terceros por un médico de dos interrupciones de embarazo, "*Se trata de un delito especial propio, con el elemento especial de autoría derivado de la exigencia de que el autor sea profesional, esto es que realice una actividad con carácter público y jurídicamente reglamentada. La acción consiste en divulgar secretos de otra persona con incumplimiento de su obligación de sigilo, tal obligación viene impuesta por el ordenamiento, Ley General de Sanidad 14/1986, de 25 de abril, cuyo artículo 10.3 estable el derecho de los ciudadanos «a la confidencialidad de toda la información relacionado con su proceso y con su estancia en instituciones sanitarias» y concurrente en el historial clínico-sanitario, en el que deben «quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica» (art. 6.1)*".

A su vez, el artículo 44 de la LOPD tipifica como infracción administrativa leve, grave o muy grave, el incumplimiento del deber de secreto profesional.

14. "El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años."

E. Prohibición de uso para finalidades incompatibles.

Establece el artículo 4.2 LOPD que *los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*. La Sentencia de la Audiencia Nacional, de 12 de junio de 2007 –JUR/2007/199159-, elabora el siguiente concepto de "fines incompatibles":

"En conclusión, si la recogida o entrega de datos de carácter personal se realizó con unos fines determinados, cualquier uso o tratamiento posterior que no esté en consonancia con las finalidades para las que fueron facilitados y sobre las que el afectado no consintió, es incompatible con la finalidad que determinó la entrega, utilizando la LOPD la expresión finalidades incompatibles como sinónimo de finalidades distintas."

Son fines compatibles, por ejemplo, la asistencia sanitaria al paciente y los estudios epidemiológicos, pero son fines distintos, por lo que es necesario, como veremos, el consentimiento del paciente o la disociación de los datos anonimizándolos.

5. EL ACCESO DEL PACIENTE Y USUARIO A SUS DATOS DE SALUD Y LA DISPONIBILIDAD SOBRE LOS MISMOS.

1. El alcance del derecho de acceso a los datos.

El artículo 18.1 LBAP y el artículo 64 de la Ley Foral 17/2010, de 8 de noviembre, establecen que el paciente tiene derecho de acceso, con las reservas que comentaré, a la documentación de

la historia clínica y a obtener copia de los datos que figuran en ella.

Además, en la normativa autonómica nos encontramos con especificaciones que suponen un avance sustancial al respecto. Así, el artículo 31.1 de la Ley Foral 17/2010, de 8 de noviembre, añade el derecho "*a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos, salvo en caso de uso codificado de los mismos*". Así pues, el derecho se extiende a conocer no solo sus propios datos de salud, sino a conocer también las personas que han accedido a esos datos.

Sin embargo, el artículo 15.1 de la LOPD, establece que el interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Es decir, solo a sus propios datos, no a datos atinentes a terceras personas. Es más, la Agencia Española de Protección de Datos, en su informe 167/2005 se muestra contraria a que se pueda acceder a conocer las personas que han accedido a sus datos. Dice este informe que "*el derecho concedido al interesado por la Ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de organización del responsable del fichero han podido tener acceso a dicha información*" Justifica este aserto señalando que esos datos serían datos de carácter personal, que deberían contar con su consentimiento, o encontrarse habilitada por ley la posibilidad, lo que no debe sucede en este caso dado el alcance que la LOPD otorga al derecho de acceso. Este mismo criterio lo reitera en su informe 171/2008.

Apuntándose a este criterio, el artículo 19.2 del Decreto 24/2011, de 12 de abril, de la documentación sanitaria en Castilla-La Mancha, establece que "El derecho de acceso del paciente a los datos de su historia clínica no comprende la información sobre los datos personales de las personas que, dentro del ámbito de la organización del responsable del fichero, han podido tener acceso a la misma en ele ejercicio de su funciones".

Así pues, extender el derecho a conocer las personas que han accedido a los datos de salud no es una cuestión doctrinalmente pacífica, aunque la doctrina se inclina mayoritariamente por que se permita al interesado el conocimiento de las personas que han accedido a sus datos de salud[15].

En mi opinión, la posición que mantienen la Agencia Española de Protección de Datos y Castilla-La Mancha a través del Decreto 24/2011, de 12 de abril, tiene escaso sustento jurídico y legal, pues se opone a la legislación de la Unión Europea y de España sobre transparencia en la Administración, que pretende asegurar el acceso por la persona a todos los datos existentes en los archivos y expedientes administrativos respecto de los que ostenten un interés legítimo, y ese interés legítimo se manifiesta paradigmáticamente en los datos obrantes en expedientes personalísimos como lo es la historia clínica. La legislación de transparencia contempla excepciones muy justificadas al acceso, pero, en mi criterio, ninguna es aplicable el caso que nos ocupa. Por tanto, considero más acertado lo dispuesto en el artículo 31.1 de la Ley Foral 17/2010, de 8 de noviembre.

15. Véase al respecto, GALLEGO RIESTRA, S. y RIAÑO GALÁN, I., "¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica?, Revista Derecho y Salud, volumen 22, núm. 1, 2012, pp. 85 a 96.

2. Capacidad. La cuestión del menor de edad.

El artículo 23 del Reglamento de la LOPD atribuye el ejercicio del derecho de acceso a la persona física titular de los datos objeto de tratamiento y reconoce expresamente su carácter personalísimo, lo que significa que debe ser ejercido exclusivamente por el titular, sin perjuicio de los supuestos de representación legal o voluntaria. En el caso de la representación voluntaria, el artículo 23 exige que quede claramente acreditada la identidad del representado y la representación conferida. Exige, además, que el representante ha de ser designado expresamente para el ejercicio de este derecho[16].

El Reglamento de la LOPD no exige la acreditación de un concreto interés legítimo para el ejercicio del derecho de acceso a los datos personales.

La cuestión del menor de edad.

La LBAP prevé tres niveles de madurez en los menores de edad conforme a la legislación civil (menores de 18 años). En el caso de personas con 16 años se les reconoce plena capacidad y no cabe el consentimiento por representación (mayoría de edad sanitaria). Entre los 12 años y los 16 se estará al criterio de capacidad natural (madurez intelectual y emocional), presumiéndose la madurez en los que han cumplido 14 años. Por debajo de los 12 años es siempre necesaria la conformidad de los padres o tutores. El artículo 9.3.c), in fine, dispone que sólo en caso de actuación

16. No valen, pues, los poderes generales para pleitos.

de grave riesgo en el menor maduro, según el criterio del facultativo, se informará a los padres y su opinión será tenida en cuenta.

El Convenio de 4 de abril de 1997 para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina, hecho en Oviedo y ratificado por instrumento de 23 de julio de 1999, en su artículo 6.2 establece que "*La opinión del menor será tomada en consideración como un factor que será tanto más determinante en función de su edad y su grado de madurez*".

Por su parte, la LOPD apuesta por llevar hasta sus últimas consecuencias la previsión contenida en la Ley Orgánica 1/1996, de 8 de enero, sobre protección jurídica del menor, haciéndole titular de su derecho al acceso y a consentir de forma autónoma el tratamiento de sus datos a partir de los 14 años (artículo 13 del Reglamento de la LOPD), criterio éste tradicionalmente sustentado por la Agencia Española de Protección de Datos también en relación con el derecho de acceso a la historia clínica (Informe 409/2004).

Y es que, en el ámbito de la protección de datos personales se ha interpretado tradicionalmente que los mayores de catorce años tiene madurez suficiente para otorgar su consentimiento para el tratamiento de sus datos personales, así como para ejercitar derechos[17]. En efecto, establece el artículo 13 del Reglamento de la LOPD sobre el consentimiento para el tratamiento de datos de menores de edad lo siguiente:

17. En este mismo sentido, informe 409/2004 de la Agencia Española de Protección de datos.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

Este es, como he dicho, el criterio de la Agencia Española de Protección de Datos desde su informe 409/2004, basándose en el artículo 162.1 del Código Civil, que excluye de la representación legal de la patria potestad los actos relativos a los derechos de personalidad u otros que el hijo, de acuerdo con las leyes y sus condiciones de madurez, pueda realizar por sí mismo.

Es también el criterio adoptado por algunos servicios Autonómicos de Salud, como, por ejemplo, el de Castilla-La Mancha, a través de la circular 1/2009, de 27 de febrero.

Así pues, el régimen parece bastante claro. En el caso de un menor mayor de 14 años, tiene pleno derecho de acceso a sus datos sin consentimiento de sus padres, y, además, un tercero, aunque sean los padres, no puede acceder a sus datos e historia clínica sin su previo consentimiento. La legislación de protección de datos no hace otra cosa que concretar lo que con carácter general establece el artículo 162.2 del Código Civil. En consecuencia, el médico no podrá informar a los padres de la atención prestada al hijo, pues vulneraría el derecho del menor maduro a la confidencialidad e incurriría en violación del deber de secreto profesional. El conocimiento de los datos de salud contenidos en la historia clínica por los padres o el representante queda limitado a los supuestos en que legalmente tenga que completar o sustituir

la capacidad. Son los casos de transplante de órganos, esterilización, cirugía transexual, ensayos clínicos, aborto, etc.

Sin embargo, esta interpretación no es pacífica. También se postula el derecho de los padres de menores de entre 14 y 16 años a conocer para poder ejercer correctamente sus obligaciones, y así lo viene disponiendo alguna normativa autonómica, que exige que el acceso de los menores de 16 años a sus datos de salud requerirá la autorización expresa de sus progenitores (artículo 12.4 del Decreto 38/2012, de 13 de marzo, del País Vasco, de derechos y deberes en materia de documentación clínica).

En el ámbito de las decisiones judiciales cabe citar la sentencia del Tribunal Superior de Justicia de Cataluña, de 7 de abril de 2010 –JUR/2010/123938–, que anula el artículo 33 del Código de Deontología Médica porque impide que los padres sean informados cuando el médico considere que el menor tiene madurez suficiente y hace prevalecer la voluntad del menor de que sus padres no sean informados.

La normativa foral nada dispone respecto de esta concreta cuestión, por lo que será de aplicación directa el artículo 13 de reglamento de la LOPD.

3. Procedimientos o fórmulas de acceso.

El citado artículo 18.1 también obliga a los centros sanitarios a regular el procedimiento que garantice la observancia del derecho de acceso. Por su parte, el artículo 64.1 de la Ley Foral 17/2010, de 8 de noviembre, establece que corresponde a la Administración regular el procedimiento que garantice el ac-

ceso. Hasta el momento, la Administración de la Comunidad Foral no ha regulado dicho procedimiento.

En todo caso, conforme a los artículos 23 a 30 del Reglamento de la LOPD el acceso se hará a través de las siguientes formas:

- El acceso ha de ser ejercitado por el interesado acreditando su identidad, o por representación voluntaria o legal (incapaces, incapacitados). Las solicitudes de acceso deben contener las menciones mínimas exigidas por el artículo 25 del Reglamento de la LOPD[18].

- Debe permitirse al interesado su derecho de acceso a través de los servicios de atención al paciente de los centros sanitarios (art. 24.4).

- Las solicitudes de acceso deben ser resueltas en el plazo máximo de un mes a contar desde la fecha de su recepción, y hacerse efectivas en la propia respuesta o en el plazo de los diez días siguientes (art. 29).

18. a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

- El acceso a la historia clínica debe articularse de forma sencilla y a través de un procedimiento gratuito sin que, en ningún caso, pueda suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan (artículo 23.4). De conformidad con la Ley Foral 11/2007, de 4 de abril, de la Administración electrónica, el paciente tiene el derecho a relacionarse con la Administración sanitaria y los centros sanitarios utilizando medios electrónicos, que comprende recabar informaciones, realizar consultas, formular solicitudes y obtener copias electrónicas. Así pues, el interesado puede optar por recibir la información mediante visualización en pantalla, escrito, copia o fotocopia remitida por correo certificado o no, correo electrónico o cualquier otro sistema adecuado a la configuración o implantación material del fichero (art. 28).

- El derecho de acceso sólo puede ser ejercido en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo, en cuyo caso podrá ejercerlo antes. El problema es que resultará complejo determinar cuando hay un interés legítimo y cuando no.

4. Límites al acceso.

El derecho de acceso del paciente o usuario a la información contenida en la documentación de la historia clínica tiene unos límites fijados por el artículo 18 LBAP. Son los siguientes:

a) No comprende los datos confidenciales de terceras personas incorporados a la historia clínica en interés tera-

péutico del paciente (un tercero que actúa en beneficio del paciente: por ejemplo, la declaración de la esposa de que el marido bebe alcohol en exceso).

b) Los profesionales participantes en su elaboración pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas (artículo 18.3 LBAP y artículo 64.3 de la Ley Foral 17/2010, de 8 de noviembre).

El apartado 4 del citado artículo 64 define el concepto de "anotaciones subjetivas" en los siguientes términos:

"*A los efectos de lo dispuesto en la presente Ley Foral, se entenderán por anotaciones subjetivas las impresiones o valoraciones personales de los profesionales sanitarios no sustentadas directamente en datos objetivos o pruebas complementarias y que, en su criterio, resulten de interés para la atención sanitaria del paciente. Se considerarán anotaciones subjetivas únicamente aquellas que puedan encuadrarse en algunos de los siguientes apartados:*

- *Valoraciones sobre hipótesis diagnósticas no demostradas.*

- *Sospechas acerca de incumplimientos terapéuticos.*

- *Sospechas de tratamientos no declarados.*

- *Sospechas de hábitos no reconocidos.*

- Sospechas de haber sido víctima de malos tratos.

- Comportamientos insólitos.

Los profesionales sanitarios deberán abstenerse de incluir expresiones, comentarios o datos que no tengan relación con la asistencia sanitaria del paciente o que carezcan de valor sanitario".

c) Aunque no aparece formulada expresamente entre los límites establecidos por el artículo 18 LBAP, también puede limitarse el acceso del paciente o usuario a la información sanitaria cuando se acredite la existencia de un estado de necesidad terapéutica, es decir, cuando se entienda que el conocimiento de determinados datos de su salud puede ser gravemente perjudicial para el paciente. Se fundamenta en el artículo 5.4 de la LBAP que contempla el estado de necesidad terapéutica. En efecto, se producen casos excepcionales en los que, por razones objetivas, el conocimiento de su situación por parte de una persona pueda perjudicar de manera grave a su salud.

5. Derecho a la rectificación, a la cancelación y a la supresión de los datos de salud. La conservación de la historia clínica.

El derecho de rectificación enlaza directamente con la obligación que tiene el responsable del fichero de mantenerlo actualizado. Puede ser definido como la facultad que tiene el interesado, una vez que ha constatado que un dato es incorrecto

o inexacto, de exigir que el responsable proceda a adecuarlo a la realidad, lo cual supone una diferencia con el derecho de cancelación, en el sentido de que, la persona que ejercita la rectificación, no persigue la supresión de datos, sino que sigan recogidos en un determinado fichero, aunque no en las mismas condiciones que estaban. La cancelación tiene como objetivo la eliminación de los datos de la historia clínica que resulten inadecuados o excesivos.

Conforme al artículo 16 LOPD, el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. La cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo debe procederse a la supresión.

El artículo 32 del Reglamento de la LOPD y la Instrucción 1/1998, desarrollan el procedimiento a seguir, que conforme al artículo 17.2 LOPD es gratuito, cuando el acceso a los ficheros revelare que los datos son inexactos o incompletos, inadecuados o excesivos, el interesado, podrá solicitar, del responsable del fichero, la rectificación, o en su caso cancelación de los mismos.

El artículo 23 de la Ley Orgánica 2/2010, de 3 de marzo, de Interrupción Voluntaria del Embarazo, dispone que los centros que hayan procedido a una interrupción voluntaria de embarazo deben cancelar de oficio la totalidad de los datos de la paciente

una vez transcurridos cinco años desde la fecha de alta de la intervención, si bien, la documentación clínica puede conservarse cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, en cuyo caso se procederá a la cancelación de todos los datos identificativos de la paciente y del código que se le hubiera asignado como consecuencia de lo dispuesto en los artículos anteriores. Añade que lo dispuesto se entenderá sin perjuicio del ejercicio por la paciente de su derecho de cancelación, en los términos previstos en la LOPD.

Señalar también que la Ley Foral 16/2010, de 8 de noviembre, que crea el Registro de profesionales objetores de conciencia, impide la cancelación de la declaración y la oposición a su tratamiento. Estas limitaciones derivan directamente de la Ley Orgánica 2/2010, de 3 de marzo, ha de entenderse proporcionada en cuanto la Administración sanitaria ha de conocer siempre y con carácter previo la condición de objetor para poder organizar adecuadamente los servicios asistenciales y garantizar una prestación de calidad a la que viene obligada. Por tanto, el ejercicio por el objetor de sus derechos a la cancelación de los datos registrados o de oposición a su tratamiento, llevaría aparejada la pérdida de la condición de objetor.

Respecto de la conservación de datos personales, la legislación sanitaria contiene una regulación específica.

Dispone el artículo 17 LBAP que:

> *1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que ga-*

ranticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

A su vez, el artículo 61.1 de la Ley Foral 17/2010, de 8 de noviembre, dispone lo siguiente:

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial.

2. En cualquier caso, en la historia clínica deben conservarse, junto con los datos de identificación del paciente, durante cinco años, como mínimo, a contar desde la muerte del paciente: las hojas de consentimiento informado, los informes

quirúrgicos y el registro de parto, los datos relativos a la anestesia, los informes de exploraciones complementarias y los informes de necropsia.

3. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Por tanto, el paciente o los familiares del paciente fallecido no puede exigir la supresión de sus datos de salud cuando pueda causarle un perjuicio o a un tercero o cuando no haya transcurrido el plazo mínimo fijado por la legislación citada –cinco años-. Transcurrido ese plazo, los datos no se destruyen sino que se bloquean según dispone el artículo 16.3 LOPD, conservándose únicamente a disposición de los Administraciones Públicas y Jueces para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Sólo cumplidos los plazos de prescripción de la responsabilidad se procederá a su definitiva supresión.

El artículo 63 de la Ley Foral 17/2010, de 8 de noviembre, establece que "*Reglamentariamente se establecerá el procedimiento para la destrucción de las historias clínicas en aquellos casos en los que se contemple legalmente así como para la conservación de los datos que pudieran ser relevantes para estudios posteriores por su importancia desde el punto de vista científico*". Todavía no se ha hechos este reglamento. Se

trataría de reglamentar un proceso de espurgo de la documentación clínica al objeto de destruir, una vez transcurridos los plazos fijados en el citado artículo 61.1, los documentos que procedan por considerarse irrelevantes o poco relevantes, enumerándose expresamente los datos o documentos que se entienden relevantes a efectos de su conservación por razones científicas, epidemiológicas, u otras justificadas que, obviamente, no serán destruidos, aunque se anonimizarán siempre que sea posible.

6. EL ACCESO A LOS DATOS DE SALUD POR PERSONAS DISTINTAS AL INTERESADO (CESIÓN O COMUNICACIÓN DE DATOS).

1. Régimen general de la comunicación o cesión de datos.

El artículo 3, apartado i, de la LOPD define la cesión o comunicación de datos como toda revelación de datos realizada a una persona distinta del interesado. A su vez, el artículo 11.1 de la LOPD sienta la regla general de que la comunicación de datos a un tercero requiere el previo consentimiento del interesado. Ahora bien, seguidamente, en el apartado 2 de ese artículo 11 precisa que no será necesario el consentimiento:

a) Cuando la cesión está autorizada en una ley.

b) Cuando la comunicación que deba efectuarse tenga por destinatario a los Defensores del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas estatal o autonómicos, en el ejercicio de las funciones que tiene atribuidas.

c) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

d) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Por su parte, el artículo 16 de la LBAP complementa lo dispuesto en el artículo 11 de la LOPD permitiendo el acceso por terceras personas a la historia clínica en los siguientes términos:

a) Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

b) Para el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se remite a lo dispuesto en la LOPD y en la Ley General de Sanidad, pero añadiendo que el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

No obstante, este artículo exceptúa de la disociación de los datos los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales. También exceptúa de la disociación el acceso por las Administraciones sanitarias a las que se refiere la Ley 33/2011, General de Salud Pública, en los casos en los que sea necesario para la prevención de un riesgo o peligro grave para la salud de la población.

c) El personal de administración y gestión de los centros sanitarios puede acceder sin previo consentimiento a los datos de la historia clínica relacionados con sus propias funciones.

d) El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

Este es el régimen general de acceso a los datos de salud de un sujeto por terceras personas. Como puede observarse, son muchas las excepciones a la regla general de previo consentimiento del interesado. Obviamente, estas excepciones traen causa de otros bienes, derechos a valores a proteger, frente a los cuales el derecho a la protección de los datos personales ha

de ceder total o parcialmente. Ahora bien, la LBAP también sienta una regla general en la cesión de datos a terceras personas, y es la regla de la disociación de los datos personales de los clínico-asistenciales, salvo que sea estrictamente necesario el conocimiento de la identidad del titular de los datos por razones judiciales o de salud pública.

La LOPD define como dato personal cualquier información concerniente a las personas físicas identificadas o identificables y como procedimiento de disociación todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona identificada o identificable. Complementa el Reglamento de la LOPD estas definiciones diciendo que dato disociado es aquél que no permite la identificación de un afectado o interesado, y que una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados. Por su parte, la Ley 14/2007, de 3 de julio, de Investigación Biomédica, define la anonimización como el proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Así pues, para considerar jurídicamente disociado o anonimizado un dato personal no es preciso que la disociación sea totalmente irreversible, sino que exija esfuerzos informáticos desproporcionados.

Entiendo que para realizar el proceso de disociación o anonimización de datos de salud a efectos de su cesión a terceros en los casos admitidos por la LOPD y la LBAP no es necesario previo consentimiento del afectado. Conforme dispone el artículo 11.6 de la LOPD, si la comunicación se efectúa tras un procedimiento de disociación, no es aplicable lo establecido en

los apartados anteriores de dicho artículo, por lo que es indiferente que exista o no consentimiento del interesado para la comunicación o cesión de datos de salud disociados por la sencilla razón de que esos datos son totalmente anónimos.

Además, junto a la eliminación u ocultación de los datos personales, también es posible instrumentar medios o técnicas para impedir el acceso y el conocimiento de concretos datos de salud. En efecto, una medida de protección de datos de salud en los supuestos en que está permitido legalmente el acceso a terceras personas sin previa disociación de los datos personales, es la de fijar perfiles de acceso en atención a la cualidad de la persona que accede y de los motivos del acceso. La informática permite hoy crear claves de acceso y perfiles profesionales de acceso por bloques de patologías, especialidades médicas, grupos de datos necesarios a efectos de inspección, facturación, estadísticas, etcétera, de manera que solo se acceda a aquellos datos estrictamente necesarios para el correcto ejercicio de la función que corresponde realizar al que accede.

En este sentido, la Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid, señaló que "Los profesionales asistenciales que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica completa de éste, como instrumento fundamental para su adecuada asistencia", y que "El personal de administración y gestión de los centros e instituciones sanitarias sólo podrá acceder a los datos de la historia clínica relacionados con sus propias funciones que podrán estar relacionadas por ejemplo, con la admisión del paciente, cita previa, funciones contables y presupuestarias. No obstante, le corresponderá a la Comunidad de

Madrid establecer a través de la ley, el procedimiento de adaptación y diferenciación de accesos a la historia clínica." Sin embargo, en mi criterio, un traumatólogo que ha de curar un esguince de tobillo no necesita para nada acceder a datos obstétricos de la paciente tales como que ha tomado cuatro veces la píldora poscoital o que ha tenido un aborto, por lo que incluso a los profesionales sanitarios que asisten directamente al paciente puede restringirse el acceso a partes de la historia clínica. Y lo que, si duda, sería totalmente improcedente es el acceso indiscriminado a la totalidad de los datos incorporados en la historia clínica por parte del personal auxiliar, administrativo, de gestión, etcétera.

También pueden establecerse mecanismos que permitan al paciente o usuario determinar un módulo de información clínica que contenga datos considerados de especial custodia en áreas tales como la genética, sexualidad y reproducción, psiquiatría, trasplante de órganos, enfermedades infecciosas, etcétera, que puedan perjudicar su vida social o laboral.

En cualquier caso, la disociación de datos, la creación de perfiles profesionales de acceso, la determinación de módulos de datos de especial custodia, etcétera, exige elaborar los correspondientes programas informáticos, programas muy complejos de implantar y aplicar. Además, debe aprobarse la correspondiente normativa que obligue jurídicamente a su utilización y que dé seguridad jurídica en su uso. Es, por tanto, indispensable y urgente que el Gobierno de Navarra apruebe la reglamentación que regule todas estas técnicas de forma que sean públicas y vinculantes jurídicamente, y que su aplicación pueda ser exigida por los centros sanitarios y por los pacientes y usuarios.

De todos modos, en este ámbito de la cesión, comunicación y acceso por terceras personas a los datos de salud de un sujeto, en la práctica diaria se produce una casuística tal que no es posible encontrar siempre una respuesta o solución al caso en la normativa vigente. De ahí que sean bastante frecuentes las consultas a la Agencia Española de Protección de Datos e innumerables los informes emitidos por la Agencia tratando de sentar criterio y dar respuesta al caso que se le ha planteado.

En dicha casuística siempre se enfrentan el derecho del sujeto a la protección de su datos de salud y otros derechos o bienes también merecedores de protección, como el derecho a la protección de la salud en su vertiente individual (familiares u otras personas) o colectiva (la salud pública), el derecho a la tutela judicial efectiva, la buena y eficiente gestión y administración de centros sanitarios, la investigación médica o epidemiológica, la docencia, etcétera. Y en este contexto ha de tenerse muy presente que el derecho que nos ocupa no necesariamente ha de prevalecer sobre otros derechos o valores que también merecen la misma o más protección. El Tribunal Constitucional reiteradamente ha señalado que "el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho." (Por todas, STC 186/2000, de 10 de julio).

Es preciso, por tanto, cohonestar medidas de protección de intereses públicos con el derecho a la intimidad de las personas

afectadas, y según la STC 186/2000 ponderar adecuadamente y de forma equilibrada "de una parte, la gravedad de la intromisión que comporta en la intimidad personal y, de otra parte, si la medida es imprescindible para asegurar la defensa del interés público que se pretende proteger". Conforme al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950, los límites a los que cualquier injerencia debe quedar sujeta son los siguientes: tener una base legal, perseguir un fin legítimo y ser una medida necesaria en una sociedad democrática, esto es, que esté justificada en aras al interés general y que las razones de su existencia sean suficientes, convenientes y convincentes (STSJ de Galicia de 16 de enero de 2008 –RJCA/2008/700-).

Un ámbito en el que es frecuente la colisión de derechos es el de los datos genéticos. Son, por ejemplo, los casos de determinación de la maternidad o paternidad, o la realización por una persona de un test genético del que resulta una predisposición familiar a padecer una determinada enfermedad. Otro ámbito es el de personas portadoras de enfermedades infecciosas. Y no es lo mismo acceder al dato genético para que un hijo pueda conocer la identidad de su madre, o para conocer la prevalencia familiar a padecer una determinada enfermedad, o para cobrar una póliza de seguro, o para acceder a un puesto de trabajo. Por ello, en la abundante casuística que puede presentarse, siempre hay que hacer una ponderación de los intereses enfrentados, particulares o públicos. La aplicación del principio de proporcionalidad es esencial en esa ponderación.

En mi criterio, no creo que deba plantearse duda alguna de que el interés público (razones de salud pública, de investigación bio-

médica, etcétera) subyacente en el acceso por un tercero (no una persona cualquiera, sino profesionales sanitarios sujetos al deber de secreto profesional) a datos de salud de un sujeto, incluso conociendo su identidad cuando sea estrictamente preciso, debe prevalecer sobre el derecho del sujeto a la ocultación de sus datos de salud. Tampoco, en mi criterio, debe impedirse el acceso por un familiar al conocimiento de un dato de salud de otro familiar del que se evidencie una clara predisposición familiar a padecer una enfermedad grave. Por el contrario, no sería proporcional ni justificado permitir el acceso si solo se trata de una enfermedad leve. Tampoco parece proporcional hacer uso de datos genéticos como medio de selección de personal.

Así, habrá de ponderarse cada caso que se presente aisladamente. En suma, en la abundante casuística que se produce en la cesión, comunicación y acceso por terceros a datos de salud de un sujeto sin su consentimiento expreso y sin que sus datos personales se hayan disociado de los clínico-asistenciales, ha de hacerse siempre una adecuada ponderación de los intereses en juego, adoptando una decisión proporcionada al logro del legítimo fin pretendido.

Respecto al juicio de proporcionalidad, la Sentencia del Tribunal Superior de Justicia del País Vasco, de 30 de noviembre de 2009 –RJCA/2010/351-, resolviendo un supuesto de comunicación de datos de salud, señala que el juicio de proporcionalidad que ha de hacerse requiere la constatación de que la medida restrictiva adoptada cumple los tres requisitos siguientes: que la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad); que sea además necesaria, en el sentido de que no exista otra medida más moderada para la consecución

del tal propósito con igual eficacia (juicio de necesidad); y, finalmente, que la medida adoptada sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en un juicio estricto de proporcionalidad (SSTC 281/2006, de 9 de octubre y STC 207/1996, de 16 de diciembre).

2. El Registro de accesos.

Con el objeto de controlar los accesos a los datos de salud por terceras persona, cuestión muy preocupante particularmente cuando se trata de historias clínicas electrónicas, el artículo 103 del Reglamento de la LOPD establece que "*De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido*".

Según el informe de la Agencia Española de Protección de Datos 0584/2009, interpretando el artículo 103, el control de los accesos deberá efectuarse de la forma más detallada posible, a fin de conocer efectivamente quién ha podido en cada momento conocer los datos incorporados al sistema, es decir, a qué datos o recursos se ha accedido, sin que puedan efectuarse meros controles genéricos, por referencia al sistema en conjunto. Por consiguiente, el responsable del fichero debe contar con las aplicaciones informáticas necesarias que permitan cumplir con las exigencias establecidas en el artículo 103 del Reglamento de la LOPD.

De cada acceso ha de guardarse, como mínimo, la identificación de la persona que accede, la fecha y hora del acceso, el fichero accedido, el tipo de acceso y si se ha autorizado o denegado. Debe existir, por tanto, un registro de accesos, que ha de conservarse, al menos, durante dos años.

La Agencia Española de Protección de Datos, interpretando en el citado informe 584/2009 el artículo 103, señala que "El aspecto esencial a tener en consideración en estos casos será el que la información almacenada en el registro de accesos permita identificar inequívocamente qué persona ha tenido acceso y a qué información contenida en el fichero en cada momento, a fin de que, en caso de ser necesario reconstruir cuándo y cómo se produjo una determinada revelación de un dato, sea posible identificar la persona que pudo conocerlo en ese momento concreto."

No es necesario registrar los accesos cuando el responsable del fichero es una persona física y garantiza que únicamente él tiene acceso y trata los datos de salud. Esta excepción es particularmente aplicable a los médicos con consulta privada.

3. El acceso por parte de familiares.

De entrada, los familiares no tienen derecho de acceso a la historia del paciente salvo consentimiento expreso de este. Cuando fallezca el paciente podrán acceder salvo expresa prohibición del mismo.

Se ha de entender por familiar la pareja, hijos, padres y hermanos. Por el contrario, a los tíos, primos, etc., salvo excepciones,

se les ha de dar la consideración de terceros más que la de familiares.

En todo caso, el acceso de un familiar a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. Colisionan aquí dos derechos: el derecho del titular de la historia clínica a la intimidad de sus datos de salud y el derecho a la integridad física de quien, estando su salud en riesgo, precisa del conocimiento de cierta información contenida en al historia clínica de otra persona y que puede ser decisiva para su diagnóstico y tratamiento. Problema realmente difícil de resolver en la práctica por lo parca que ha sido la LBAP al respecto. Es decir, la legislación no da una respuesta clara a esta problemática.

Y, en efecto, en el ámbito familiar, con frecuencia, se plantean problemas de difícil resolución. Como muestra, cabe traer a colación los test genéticos. Es el caso, por ejemplo, de una paciente que se ha sometido a un test genético para conocer su predisposición a sufrir un cáncer de mama. Si resulta positivo significa que los familiares también tienen esa predisposición. Entonces, el dilema de los médicos es si deben informar a los familiares de esa circunstancia a fin de prevenir esa enfermedad o si debe prevalecer el derecho de la paciente a la protección de sus datos si se niega a que se facilite ese dato. Las posiciones son encontradas. Un sector defiende que debe facilitarse la información a los familiares pues prevalece el derecho a la vida sobre el derecho a la intimidad, y otro sector considera que debe ocultarse esa información a los familiares si no la consiente el paciente. Mi posición al respecto ya la he manifestado anteriormente en el punto 1.

Es también el caso de los enfermos de SIDA o de otro tipo de enfermedades infecciosas altamente trasmisibles. Buena parte de la doctrina es favorable al acceso de los datos entendiendo que el principio de solidaridad exige el sacrificio del derecho a la intimidad en función de la garantía del derecho a la salud de la colectividad. Esta posición ha sido avalada por la jurisprudencia (por ejemplo, STSJ de Asturias de 12 de septiembre de 2005).

4. El acceso por parte de terceros o del público en general.

El artículo 11.1 LOPD establece que los datos de carácter personal objeto de tratamiento solo pueden ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Cada vez es más frecuente la externalización del tratamiento de datos. La informatización de las historias clínicas se suele realizar con el apoyo de empresas externa, que, por tanto, hacen el tratamiento de los datos de salud. Contemplando esta realidad, el artículo 12.1 LOPD dispone que "No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento." Seguidamente, el artículo 12.2 señala que "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin

distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas[19].”

Un ámbito en el que es frecuente la necesidad de cesión de datos a terceros es el generado por accidentes de circulación. El informe 114/06 de la Agencia Española de Protección de Datos considera que hay habilitación legal suficiente para que los centros sanitarios públicos y privados y las Mutuas Patronales de Accidentes de Trabajo y Enfermedades Profesionales entreguen a las entidades aseguradoras, sin consentimiento del paciente, determinados datos referidos a la asistencia sanitaria a efectos de facturación, si bien entiende que a las compañías de aseguramiento privado únicamente se les puede facilitar aquellos datos de la historia clínica imprescindibles a efectos de facturación del gasto sanitario efectivamente llevado a cabo. Así pues, exclusivamente los que sean imprescindibles para la finalidad perseguida. Cualquier otra información clínica solicitada por la compañía aseguradora requerirá el consentimiento expreso del paciente.

En lo que hace a personajes de relieve público, según doctrina del Tribunal Constitucional la libertad de información prevalece sobre la intimidad personal siempre que la comunicación a la opinión pública esté justificada por razón de interés público. La doctrina jurídica del Tribunal Constitucional y del Supremo define como personas públicas a aquéllas de "relevancia social e interés informativo". Incluso el Tribunal Europeo de Derechos Humanos mantiene el criterio de "que sobre los he-

19. El informe 177/2010 de la Agencia Española de Protección de Datos hace un detenido estudio sobre la forma en que se pueden externalizar el servicio de tratamientos de datos personales.

chos que tienen interés público prima el derecho de la información sobre el del honor y que son personajes que tienen que soportar un plus de intromisión en su vida privada[20]".

5. El acceso por facultativos sanitarios.

La LBAP reconoce el derecho a acceder a la información contenida en las historias clínicas, sin necesidad de consentimiento del paciente, a los profesionales asistenciales que realicen el diagnóstico y el tratamiento (art. 16.1). Por tanto, han de ser facultativos vinculados asistencialmente con el paciente. El acceso por otros facultativos del centro no vinculados asistencialmente al paciente, de entrada, debe estar muy restringido. A efectos de investigación, etc., podrán acceder pero una vez que estén disociados los datos.

Conforme al artículo 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, es necesario el previo consentimiento del trabajador para que las Unidades de prevención de Riesgos Laborales puedan ceder sus datos de salud a terceros, incluso a facultativos del Sistema nacional de Salud a efectos asistenciales.

Por otra parte, en la historia clínica, particularmente en la electrónica, cabe establecer determinadas restricciones a los propios facultativos sanitarios que asisten al paciente, en el sentido de solo poder acceder a los datos clínicos necesarios para el diag-

20. Resultaría interesante estudiar el caso de un político que ejerce un cargo público, que padece una adicción severa o se le diagnostica una enfermedad mental invalidante, lo que puede interferir claramente en su capacidad para gobernar. ¿Es razón suficiente para hacer públicos esos datos?

nóstico y tratamiento. Por ejemplo, el conocimiento de que el feto de una mujer embarazada sea fruto de un óvulo donado es clave para el obstetra, pero es irrelevante para cualquier otro profesional (traumatólogo ante un esguince de tobillo), y es una información muy sensible para la mujer.

El acceso a la historia clínica de los médicos internos residentes o alumnos de grado de titulaciones sanitarias, adscritos en período de formación reglada a un centro del sistema sanitario público, con finalidad docente, requiere la autorización de la dirección del centro sanitario a propuesta motivada de la persona tutora responsable de su formación.

6. El acceso por personal de enfermería, trabajadores sociales, etc.

Ha de permitirse el acceso a la información contenida en la historia clínica al personal de enfermería, auxiliar de clínica, trabajadores sociales, a fin de garantizar una asistencia al paciente (artículo 16.1 LBAP)[21].

El acceso debe estar restringido a los datos imprescindibles para el ejercicio de sus funciones en relación con su puesto de trabajo. Rige aquí el principio de proporcionalidad. Es recomendable que se fijen perfiles de acceso para cada profesional según su titulación y funciones de forma que sólo accedan a los necesarios para realizar las funciones que le son propias.

21. En este sentido, informe 656/2008 de la Agencia Española de Protección de Datos.

7. El acceso por profesionales sanitarios de centros, servicios y establecimientos concertados para la prestación de servicios.

También se debe permitir el acceso a la información contenida en la historia clínica a los profesionales sanitarios que trabajen para las personas físicas o jurídicas que presten servicios concertados en otros centros sanitarios o de Servicios Sociales de la Administración de la Comunidad Foral, previa acreditación del cumplimiento de las exigencias contenidas en la normativa de protección de datos personales. Este acceso estará limitado a las historias clínicas de los pacientes o usuario que los centros públicos remitan a los centros concertados y en el marco temporal que dure esa atención.

Igualmente, la cesión de datos al Servicio Navarro de Salud de un paciente asistido en un centro privado concertado, en el marco del concierto, debe hacerse sin necesidad de consentimiento previo del paciente. No así cuando se trata de un paciente privado fuera del marco del concierto.

Todo lo anterior por cuanto, aun no formando parte integrante del Sistema Nacional de Salud, los centros concertados desarrollan acciones asistenciales directamente vinculadas con el sistema, pudiendo incluso entenderse que las mismas constituyen, en cuanto sea objeto de concierto, servicios propios del SNS (Informe 600/2009 de la AEPD).

8. El acceso a efectos de las actividades de inspección, evaluación, acreditación y planificación sanitaria.

Conforme al artículo 16.5 LBAP, sin necesidad de consentimiento del paciente, ha de permitirse el acceso a la informa-

ción contenida en la historia clínica al personal debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, en la medida en que lo precise para el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, del respeto de los derechos del paciente o de cualquier otro deber del centro en relación con los pacientes y usuarios o la propia Administración sanitaria o de servicios sociales. El acceso mencionado tiene el alcance propio de la labor encomendada a la autoridad que accede, y debe respetar el derecho a la intimidad personal y familiar de los pacientes o usuarios.

9. El acceso a requerimiento Judicial, de la Fiscalía, del Defensor del Pueblo, del Tribunal de Cuentas y de las Fuerzas y Cuerpos de Seguridad.

Sin necesidad de consentimiento del paciente, ha de facilitarse siempre el acceso a la información contenida en la historia clínica para llevar a cabo sus investigaciones a Jueces y Tribunales, al Defensor del Pueblo, al Ministerio Fiscal y al Tribunal de Cuentas (art.11.2 d) LOPD).

La STS de 17 de noviembre de 2009 -RJ/2009/8046-, ha precisado que los términos del artículo 11.2.d) de la LOPD dejan poco espació a la duda, ya que la excepción sólo se predica de las comunicaciones de datos con los concretos destinatarios que se indican en dicho artículo, y en el ejercicio de sus funciones, lo que necesariamente implica una comunicación directa y que la misma se produzca a requerimiento del destinatario en el ejercicio de sus funciones, circunstancias que ha de valorar el responsable del fichero para emitir la correspondiente comuni-

cación de datos al amparo de dicha excepción, que, además y por su propia naturaleza, ha de interpretarse en sentido estricto. Esta interpretación le da pie al TS para concluir que la cesión de datos a los letrados intervinientes en determinados procesos judiciales a la hora de formular y proponer sus pruebas, no puede ampararse en la excepción prevista en el art. 11.2.d) de la LOPD.

La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

Incluso, sin necesidad de requerimiento judicial, debe ponerse en conocimiento del juzgado o Ministerio Fiscal los pacientes atendidos por agresiones y los casos sospechosos de abusos, incluso aunque éste no lo quiera. Y al respecto, recordemos que, según dispone el artículo 16.3 LOPD, los datos de salud, aunque hayan pasado los cinco años de conservación que exige la LBAP, han de seguir conservándose, si bien bloqueados, a disposición de los Administraciones Públicas y Jueces, para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Sólo cumplido los plazos de prescripción se procederá a su definitiva supresión.

Los Tribunales Eclesiásticos no son órganos integrados en el Poder Judicial a los efectos del artículo 11.2 LOPD, por lo que no puede cedérseles datos personales sin consentimiento del afectado[22].

10. El acceso a efectos de responsabilidad patrimonial.

En los supuestos de procedimientos administrativos de exigencia de responsabilidad patrimonial sobre la asistencia sanitaria debe permitirse que los órganos administrativos competentes para su tramitación y resolución tengan acceso a la información contenida en la historia clínica del reclamante, limitado estrictamente a los fines específicos de cada caso. Así lo prevé el artículo 16.3 de la LOPD.

11. El acceso a efectos de funciones administrativas del centro, facturación de servicios sanitarios, etc. En particular, la incorporación de datos económicos a la receta médica y a la TSI.

Autoriza el artículo 16.4 LBAP que el personal de administración y gestión de los centros sanitarios pueda acceder a los datos de salud relacionados con sus propias funciones, sin necesidad de consentimiento expreso del paciente.

Como ya he dicho antes, a las compañías de aseguramiento privado sólo se les debe facilitar aquellos datos de la historia clínica imprescindibles a efectos de facturación, con la fina-

22. En este mismo sentido, informe 611/2008 de la Agencia Española de Protección de Datos.

lidad de la justificación del gasto (accidentes de circulación, etc.). Cualquier otra información clínica solicitada por la compañía aseguradora requerirá el consentimiento expreso del paciente.

La cuestión relativa a la incorporación de datos económicos a la receta médica y a la TSI.

Como ya es bien conocido, en virtud del Real Decreto-Ley 16/2012, de 20 de abril, la aportación por los medicamentos que ahora han de hacer todos los pacientes, activos y pensionistas, pasa a ser proporcional a su nivel de renta (cantidad consignada en la casilla de base liquidable general de la declaración del IRPF). Pues bien, el nuevo art. 94 ter de la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, dispone que para determinar la cuantía de la aportación de los beneficiarios respecto de los medicamentos recetados, el Instituo Nacional de la Seguridad Social podrá recibir comunicación de la administración tributaria competente sobre los datos necesarios para determinar el nivel de renta requerido. Se cumple, pues, con el art. 1.1 de la LOPDP, que exige previsión en norma con rango de ley para eximir en la cesión de datos personales del consentimiento del afectado.

Una vez recibido el dato por la Administración tributaria, el INSS comunica a las Administraciones sanitarias el dato relativo al nivel de aportación de cada paciente, y estas lo incorporarán a la TSI mediante códigos de clasificación. A su vez, las recetas oficiales se adaptarán a distintos modelos según códigos de clasificación.

Así, el médico[23] que expide la receta oficial y el farmacéutico que dispensa el medicamento recetado, no tendrán acceso a la cuantía de la renta del interesado, pues en la TSI y en la receta médica solo figurará la clasificación establecida mediante código alfanumérico. Evidentemente, aquí ya no hay una cesión directa y concreta de datos económicos del paciente. Ahora bien, esa clasificación que sí conocerán el médico, el farmacéutico y otros (personal que gestiones las recetas), también permite conocer el tramo de renta en la que se encuentra el paciente, y, en mi criterio, es una información de carácter económico lo suficientemente relevante para requerir el previo consentimiento del paciente, o una previsión legal que exima de ese requisito. Sin embargo, el Real Decreto-Ley nada contiene al respecto, por lo que la implementación, sin más, de este sistema creo que puede suponer una vulneración del derecho a la protección de datos personales del paciente.

12. El acceso a datos de personas fallecidas.

Ya he dicho que, conforme dispone el Reglamento de la LOPD, el régimen de protección de datos de la LOPD no es de aplicación a los datos referidos a personas fallecidas. Esto trae causa de que en el derecho civil la personalidad de las personas físicas se extingue con la muerte[24]. No obstante, el Reglamento de la LOPD admite que las personas vinculadas al fallecido, por razones familiares o análogas, puedan dirigirse a los responsables de los ficheros o tratamientos para

23. El médico está autorizado a acceder y tratar la información clínica de los pacientes que tiene asignados sin su consentimiento expreso (art. 16.1 de la Ley 41/2002, de 14 de noviembre), pero solo la clínica, no la económica.

24. La STC 2000/292, de 30 de mayo, así lo contempla también.

notificar la muerte y, tras la acreditación suficiente, pedir la cancelación de los datos.

Sin embargo, en el ámbito de los datos de salud hay que estar a lo que dispone la legislación sanitaria. Así, establece el artículo 18.4 LBAP y el 67.3 de la Ley Foral 17/2010, de 8 de noviembre, que los familiares o personas vinculadas por análoga relación pueden acceder a los datos de la historia clínica del fallecido únicamente si éste no lo hubiera prohibido de forma expresa. Aun no existiendo prohibición expresa, tampoco pueden acceder en tres casos: a) información que afecte a la intimidad del fallecido; b) la que se refiera a las anotaciones subjetivas de los profesionales; c) la que perjudique a terceros.

13. El acceso con fines históricos, estadísticos, científicos, de investigación o docencia.

El acceso a la información contenida en la historia clínica con fines de investigación o de docencia se rige por lo dispuesto en la LOPD, en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso, entre otras, la Ley 12/1989, de 9 de mayo, de la función estadística pública, la Ley 13/1986, de 14 de abril, de investigación científica y tecnológica, la Ley 14/2007, de 3 de julio, de investigación biomédica.

El artículo 16.3 LBAP exige la necesaria disociación de los datos. El acceso a la información contenida en la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente o usuario, separados de los de

carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, excepto que el propio paciente o usuario diese su consentimiento para no separarlos, o bien existan criterios técnicos y/o científicos que requieran la identificación de la persona a efectos epidemiológicos y de salud pública. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos en cada caso.

El acceso a la información contenida en la historia clínica con fines de investigación se puede llevar a cabo únicamente para proyectos de investigación que sean científicamente aprobados. Esta aprobación normalmente se efectúa por el órgano de la Consejería de Salud competente en materia de investigación y a propuesta de la dirección del centro al que pertenece el investigador principal del proyecto[25].

Al objeto de garantizar la confidencialidad de la información clínica, a efectos de su difusión o publicación se han de tener en cuenta necesariamente las siguientes normas:

a) No se difundirán aquellos datos que permitan la identificación del paciente o usuario.

b) Cuando sea absolutamente necesario identificar al paciente o usuario, será preceptiva la autorización por escrito del mismo.

25. Por Orden Foral de 31 de octubre de 1991 se creó la Comisión Asesora Técnica en materia de Investigación de ciencias de la salud.

c) La difusión o publicación de resultados seguirá en todo caso las normas y sugerencias relativas a la buena práctica en investigación.

d) Cuando sea necesaria la publicación de imágenes médicas o cualquier otro soporte audiovisual que muestren partes del cuerpo del paciente o usuario, y de ellas se pudiera llegar a conocer su identidad, será obligatorio el permiso escrito del mismo.

14. El acceso con fines epidemiológicos y de salud pública.

El artículo 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, establece al respecto:

"*1. Las autoridades sanitarias con el fin de asegurar la mejor tutela de la salud de la población podrán requerir, en los términos establecidos en este artículo, a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria.*

2. Las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población.

3. A los efectos indicados en los dos apartados anteriores, las personas públicas o privadas cederán a la autoridad sanitaria, cuando así se las requiera, los datos

de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública se someterá a lo dispuesto en el apartado 3 del artículo 16 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".

El citado artículo 16.3 de la LBAP dispone que el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Es decir, procede la disociación de los datos.

Ahora bien, también dispone este precepto que "*Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el ac-*

ceso a los datos".[26] Es el caso, por ejemplo, de las enfermedades de declaración obligatoria individual, no numérica (enfermedades infectocontagiosas)[27].

26. Párrafo añadido por la Ley 33/2011, de 4 de octubre, General de Salud Pública.

27. La Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, habilita directamente a las autoridades sanitarias de las distintas Administraciones Públicas para el reconocimiento, tratamiento, hospitalización o control de personas cuando se aprecie indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad.

    Sin embargo, en estos casos el derecho a la intimidad y a la confidencialidad de los datos sanitarios con el correlativo deber de su protección no está debidamente garantizado. Se hace preciso regular adecuadamente lo relativo a la confidencialidad y protección de los datos de salud de las personas implicadas en tratamientos obligatorios por padecer enfermedades transmisibles (más cuando socialmente se siguen considerando vergonzantes). La regulación de la LOPD y de la LBAP son claramente insuficientes y no dan respuesta adecuada a estas especificidades propias del ámbito sanitario.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

Colabora:

Gobierno de Navarra