Oñati International Institute for the Sociology of Law
Instituto Internacional de Sociología Jurídica de Oñati
Oñati Socio-Legal Series
ISSN: 2079-5971
Oñati Socio-Legal Series, v. 1, n. 8 (2011) – Ancianidad, derechos humanos y calidad de vida
ISSN: 2079-5971

Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad[1]
(The technologies of the information; right to the privacy, data processing and older persons)

MARÍA NIEVES DE LA SERNA BILBAO*

Abstract

The fundamental right to the privacy consecrated in the article 18.4 of the Spanish Constitution is a guarantor institution whose objective is "to give response a new form of threat makes concrete to the dignity and to the rights of the person", but that it constitute "it self, a right or fundamental freedom". It is, it self "a right to the freedom opposite to the potential aggressions to the dignity and to the freedom of the person fro an illegitimate use of the treatment mechanized of information". Never however, in spite of the importance of this right, still it is a right little known. Less for the major person and those that represent accompany or help them. This article is focused to highlighting essential aspects of that right that must be known necessarily for the mayor person and his environments in altars to protect his intimacy and all his rights, to be or not fundamental.

Key words

Older Persons; Elderly; Right to the Protection of Personal Data; Privacy; Medical Data; Health Data; Social History; Clinical History; Assistance Centers; Centers of Major Persons; Video Vigilance; Sources Accessible to the Public

Resumen

El Derecho fundamental a la Protección de Datos consagrado en el artículo 18.4 de la Constitución Española, es un instituto de garantía que actúa *"como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona",* pero que constituye *"en sí mismo, un derecho o libertad fundamental*". Es, en sí mismo, "*…el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".* No obstante, a pesar de su importancia, aún se trata de un derecho poco conocido y, menos aún, por las personas mayores. Conocer y respetar su regulación es esencial para impedir cualquier vulneración a la dignidad, libertad y derechos de las personas mayores que, frente al uso de las tecnologías, son aún más vulnerables. De ahí, que este trabajo vaya enfocado a destacar algunos de los múltiples aspectos que es preciso conocer por las personas mayores y en aras a proteger su intimidad y todos sus derechos, sean o no fundamentales.

[1] El presente trabajo se desarrolla dentro del proyecto DER2009-09819 "De los servicios públicos y los servicios de interés general: El futuro de intervención pública en un contexto de crisis económica", dirigido por el prof. T. Quadra-Salcedo.
* Prof. Titular de Derecho Administrativo, Universidad Carlos III de Madrid, nieves.delaserna@uc3m.es[1]

Palabras clave

Personas mayores; Ancianidad; Derecho a la protección de datos; Privacidad; Datos médicos; Datos de salud; Historia social; Historia clínica; Centros asistenciales; Centros de mayores; Dependencia; Videovigilancia; Fuentes accesibles al público

Índice

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

1. Tercera edad y políticas públicas: dependencia y envejecimiento activo

1.1. Regulación y concepto

Como es sabido, las personas de la tercera edad[2] precisan de una mayor atención y una mejor información para que pueda hacerse efectivo el mandato del artículo 10 de la Constitución Española que dispone:

> "1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social.
>
> 2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y acuerdos internacionales sobre las mismas materias ratificados por España.".

Por su parte, el artículo 9.2 del citado Texto Constitucional concreta como obligación para los poderes públicos, el

> "promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas, remover los obstáculos que impidan o dificulten su plenitud".

Para lograr hacer efectivos aquellos derechos de las personas mayores, se articularon por los poderes públicos diferentes políticas públicas, entre las que cabe destacar, por su relativa novedad, la regulación sobre Dependencia y la nueva política sobre el "envejecimiento activo" [3].

En relación con la Dependencia, es preciso indicar que, tanto a nivel estatal como autonómico, se define a la misma como la situación en la que se encuentran aquellas personas que, por la falta o la pérdida de autonomía personal, necesitan asistencia o ayudas para realizar las actividades corrientes de la vida. Toda la normativa que regula la Dependencia, tiene como objetivo ofrecer y garantizar la protección a determinadas personas, entre las que se encuentran las personas mayores, que precisan una atención especializada –tanto de familiares como de personal experto-, como consecuencia de las deficiencias, enfermedades o trastornos que sufren. Principalmente, el apoyo que reciben estas personas es para poder realizar las actividades tan básicas de la vida cotidiana, como levantarse, bañarse, salir a la calle, etc. y contribuir a que éstas obtengan un mejor bienestar social mediante la prevención, la eliminación o el tratamiento de las causas que impidan o dificulten la plena integración de las personas en la sociedad[4].

---

[2] Con carácter general, se considera que una persona es mayor, cuando supera los 65 años. La Dra. María Isolina Dabove Caramuto, considera más correcto la utilización del concepto de "Ancianidad" para referirse a este grupo de personas. Dicha autora, investigadora especializada en la materia sobre ancianidad, ha publicado prestigiosos trabajos en los que explica los motivos por los que considera más apropiado el uso de éste término, frente a otros, entre los que cabe señalar, los trabajos sobre *Los derechos de los ancianos* (2005); *"Consentimiento informado y Derecho de la ancianidad: investigación, tratamientos terapéuticos en Geriátricos"* (2002, pp. 489-495); *Derecho de la Ancianidad. Perspectiva Interdisciplinaria* (2006). Igualmente, la citada profesora es Directora del Centro de Investigaciones en Derecho de la Ancianidad, vinculado a la Facultad de Derecho de la Universidad Nacional de Rosario, Argentina, Centro que desarrolla una labor importantísima en relación con el estudio y discusión sobre los distintos temas relacionados con la Ancianidad.
No obstante, los fundamentados razonamientos expresados por la autora relativos a la correcta utilización del concepto Ancianidad, en este trabajo, se utilizará el término de "personas mayores" o de "persona de la tercera edad", dado que son los que la legislación española utiliza.

[3] En el Libro Blanco de atención a las personas en situación de dependencia en España (diciembre de 2004-IMSERSO), se destacan las distintas políticas que supusieron hitos de envergadura para la mejora de la protección social en nuestro país y, consecuentemente, para las personas mayores. Por su parte, el Libro Blanco del "envejecimiento activo" en España, de 2011, es otro documento elaborado por el gobierno que tiene por finalidad servir de guía a las políticas dirigidas a mejorar la calidad de vida de las personas mayores y contiene importantes propuestas que responden a la realidad, los deseos y las expectativas de las personas mayores, contempladas con perspectiva de futuro.

[4] A nivel estatal, véase la Ley 39/2006, de 14 de diciembre, de Promoción de la autonomía Personal y Atención a las personas en situación de dependencia. En el ámbito autonómico, todas las Comunidades

Desde una perspectiva distinta a la anterior, el poder público también ha trabajado en la política denominada "envejecimiento activo", entendido como «*el proceso de optimización de oportunidades de salud, participación y seguridad con el objetivo de mejorar la calidad de vida a medida que las personas envejecen*»[5]. La citada política, recogida en el Libro Blanco sobre envejecimiento activo en España, reconoce que el aumento del número de personas mayores en nuestra sociedad –tanto a nivel español como europeo- y los cambios que dicho grupo está experimentando, han originado nuevas formas de vida de las personas mayores. Se las describe como personas activas, sanas, que se cuidan con la finalidad de ser independientes y autónomas el mayor tiempo posible y que demandan cada día más espacio y voz social. Concretamente se indica en el citado Libro que se trata de personas que *"Tienen el deseo decidido de seguir ejerciendo sus derechos de ciudadanía y de participar en todo lo que nos incumbe y atañe como sociedad. Y este hecho exige al tejido social en su conjunto responder a estas legítimas aspiraciones y a enriquecerse con ella".*

En conclusión, dentro del grupo que denominamos personas mayores o de la tercera edad, se encuentran personas en distintas situaciones. Algunas, con plena capacidad para el desarrollo de todas las actividades sin necesidad de ayudas especiales; otras, que deben recibir determinadas prestaciones por parte de los poderes públicos para lograr un grado de autonomía y desarrollo integral de la persona y, finalmente, aquellas que se encuentran en un nivel intermedio entre las dos. Desde este punto de vista, corresponde al poder público competente por medio de las instituciones administrativas habilitadas al efecto y, con fundamento en la normativa vigente, concretar qué tipo de ayudas se pueden otorgar y qué actividades se deben fomentar para logar que todas las personas mayores sean lo más independientes y autónomas posibles[6]. Para el acceso, tratamiento y uso de todos aquellos datos, la Administración utiliza las Tecnologías de la Información y la Comunicación, -más conocidas por las siglas TIC- definidas como un "conjunto de recursos necesarios para manipular los datos, información y, particularmente, los ordenadores, programas informáticos y redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla". A través de las TIC, se recaba, retiene, manipulan o distribuyen datos y se obtiene información. En todo este proceso, los datos personales recabados deben tratarse y guardarse con pleno respeto al Derecho Fundamental a la Protección de Datos, reconocido como veremos inmediatamente, en el artículo 18.4 de la Constitución Española.

1.2. Objeto del trabajo

No es posible desconocer que las personas mayores, en general, frente al uso de las TIC son reacias a su utilización cuando no temerosas a su manejo y conocimiento. Más aún, en los supuestos que se animan a utilizar las citadas tecnologías (cada día mayor número), desconocen, en gran medida, los peligros que la misma puede acarrear a la dignidad y libertad de su persona. En particular, en relación con nuestro trabajo, la dación de datos personales por parte de las personas mayores, bien sea a través del uso de las TIC, bien a instituciones –públicas o privadas- o bien a personas físicas, sin tener conocimiento del uso y el tratamiento que los datos facilitados pueden tener y, consecuentemente, los perjuicios que, en su caso, les pueden ocasionar, son en general, ignorados por

Autónomas cuentan con una regulación semejante. Al respecto, se puede consultar la página web del Instituto de Mayores y Servicios Sociales -IMSERSO -http://www.imserso.es- que contiene una relación actualizada toda la normativa sobre dependencia.

[5] Definición de la Organización Mundial de la Salud, Plan de Acción Internacional sobre el Envejecimiento: informe sobre su ejecución, 2 de diciembre de 2004.

[6] En este sentido, el Real Decreto 727/2007, de 8 de junio, que desarrolla reglamentariamente a la Ley 39/2006, concreta los criterios para determinar la intensidad de protección de los servicios y la cuantía de las prestaciones económicas, entre los que cabe citar, a) los servicios de prevención, b) los Servicios de promoción de la autonomía personal, c) la Teleasistencia, d) la Ayuda a Domicilio y e) los Centros de Día y de Noche.

este grupo de personas. Lo mismo cabe decir en relación con las distintas garantías que el sistema jurídico le reconoce para defender y proteger la recopilación y tratamiento de los datos de carácter personal, desconocimiento que también se hace extensivo a la mayoría de las personas que apoyan, acompañan o asisten a las personas mayores. El resultado de aquel desconocimiento no es otro que la inmensa posibilidad de que su Derecho a la Protección de Datos sea vulnerado.

Teniendo en cuenta lo anterior, el trabajo que se presenta pretende dar a conocer quién puede recoger los datos personales de las personas mayores, qué garantías se deben ofrecer y, por tanto, cumplir a la hora de recoger dichos datos, qué uso o destino pueden tener los datos obtenidos, qué normativa existe para legitimar su acceso, uso y tratamiento, qué personas pueden utilizarlos o quién, además de ellos, pude acceder a los datos, entre muchas otras cuestiones. En definitiva, se trata de abordar el estudio del Derecho Fundamental a la Protección de Datos, derecho que persigue proteger el denominado derecho a la privacidad. Este derecho reconocido a "todas las personas", persigue garantizar el libre desarrollo de la personalidad, al reconocer y otorgar, en nuestro caso a la persona mayor titular del dato, un poder de control y disposición sobre sus datos para preservarlos de un uso ilegítimo o no querido por parte de terceros. No obstante, es preciso indicar que excede del objetivo de este trabajo un estudio exhaustivo sobre todos los ámbitos que pueden afectar a las personas mayores. El estudio que se realiza, sólo se centra en el estudio de algunos datos que consideramos puede tener mayor repercusión en la intimidad de las personas mayores.

2. El derecho fundamental a la protección de datos

2.1. Fundamento constitucional

El Derecho Fundamental a la Protección de Datos se reconoce en la Constitución Española en el artículo 18.4 que dispone:

> "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

El constituyente, cuando incluyó este precepto, fue consciente de los riesgos que entrañaba el uso de la informática y, en tal sentido, encomendó al legislador la garantía del Derecho Fundamental a la Protección de Datos al incorporar por el mencionado artículo 18.4 del Texto Constitucional, un instituto de garantía *"como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona",* pero a la vez, considerado *"en sí mismo, un derecho o libertad fundamental"* (STC 254/1993, de 20 de julio, FJ 6). Este instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos es, para el Tribunal Constitucional, además, en sí mismo "*un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos",* que la Constitución llama "la informática'", y que el citado Tribunal ha denominado el Derecho fundamental a la Protección de Datos (STC 292/2000 de 30 de noviembre).

Por su parte, la Carta Europea de los Derechos Fundamentales, en su artículo 8, también recoge el Derecho a la Protección de datos de carácter personal, al indicar:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. 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. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

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, desarrolla este Derecho. La citada Directiva, se constituyó en el texto de referencia a escala europea en materia de protección de datos personales, al crear un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. Con este objetivo, la Directiva fijó unos límites estrictos para la recogida y la utilización de los datos personales y, además de su trasposición legislativa, exigió la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos[7]. En España, la trasposición de dicha normativa se realiza a través de la Ley orgánica 15/1999, de 15 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), norma que crea la Agencia Española de Protección de Datos de Carácter Personal, como una administración independiente.

2.2. La importancia del estudio del Derecho a la Protección de Datos en las personas mayores

Partiendo de las consideraciones anteriormente realizadas, es preciso destacar que el conocer y difundir qué supone el Derecho Fundamental a la Protección de Datos, resulta esencial para defender la libertad y dignidad, en nuestro caso, de las personas mayores. El derecho a la protección de datos, es aún, un derecho, como hemos destacado, casi desconocido por este grupo de personas a pesar del importante avance de las TIC. No obstante, el citado derecho fundamental se convierte en un elemento de garantía de importantes derechos, en especial, para las personas mayores, como la intimidad, el honor y el pleno disfrute de los restantes derechos reconocidos a los ciudadanos. Todos aquellos valores entroncan de forma directa con los principios de Democracia y Estado de Derecho, reconocidos como base de la Unión Europea en el mismo preámbulo de la Carta de los Derechos Fundamentales Europea.

Desde este punto de vista, es necesario señalar que el Derecho a la Protección de Datos debe ser conocido para impedir cualquier vulneración a los derechos. Sin embargo, es preciso indicar que en el caso de las personas mayores es igualmente importante que además de que ellas mismas lo conozcan también aquellas personas que le prestan asistencia -sean familiares o no- así como todos los que recopilan y tratan los datos de las personas mayores estén formados en esta materia. En concreto, como ya apuntamos anteriormente, en relación con nuestro trabajo, los perjuicios que puede ocasionar la dación de datos personales de las personas mayores, en general, son ignorados, al igual que las distintas garantías que el sistema jurídico le reconoce para defender y proteger su Derecho a la Protección de Datos. El resultado de aquello no es otro que una importante posibilidad de que el Derecho a la Protección de Datos se vea vulnerado.

Desde aquella perspectiva, este trabajo, pretende exponer en primer lugar, los principios y derechos que se deben conocer en relación al Derecho Fundamental a la Protección de Datos en la legislación española, para luego centrarnos en el estudio de algunos ámbitos concretos donde los datos de las Personas Mayores son tratados. Por ello, resulta necesario e imprescindible conocer los derechos que les asisten y las garantías que el ordenamiento jurídico articula en defensa del citado Derecho. En especial, nos centraremos en tratamientos tradicionales, como las historias clínicas o los datos recogidos para la prestación de los servicios sociales o la teleasistencia –aspectos muy ligados a la legislación sobre dependencia-, así como aquellos datos recogidos de los listines telefónicos, denominados por la LOPD

[7] El estudio del Derecho a la Protección de Datos, tanto a nivel español como comunitario, ha sido abordado por numerososo e importantes trabajos que resulta imposible recoger en este trabajo. Sólo se mencionan algunos en el apartado VI Bibliografía.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

como fuentes accesibles al público o los captados por los sistemas de videovigilancia.

3. El régimen jurídico de la protección de datos

3.1. Aspectos generales

Como hemos visto, el artículo 18.4 del Texto Constitucional, reconoce el Derecho Fundamental a la Protección de Datos. El citado precepto, fue desarrollado por la LOPD y, por su normativa de desarrollo, entre la que cabe destacar, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 15 de diciembre, de Protección de Datos de Carácter Personal (en adelante, RLOPD).

Con carácter general, de acuerdo con lo dispuesto por el artículo 2.3 de la LOPD, *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado",* siendo datos de carácter personal, conforme al artículo 3 a) de la misma Ley, *"Cualquier información concerniente a personas físicas identificadas o identificables"* y que el RLOPD precisa como *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*. Igualmente, el citado reglamento 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. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética"*. Sin embargo, no se consideran datos de carácter personal los datos disociados que son aquellos que *"no permite la identificación de un afectado o interesado"*

En este sentido es preciso indicar que, cuando se menciona el concepto de dato, éste 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. Así por ejemplo, se protege no sólo datos de salud sino también los datos sobre gustos o aficiones de las personas e, incluso, aquellos que puedan parecer irrelevantes para incidir en la dignidad como el color de pelo o el número de pie que se calza. Debe quedar claro que el objeto del Derecho a la Protección de Datos no es proteger la intimidad individual -para ello está la protección que otorga el art. 18.1 CE-, sino los datos de carácter personal frente a las potenciales agresiones a la dignidad y a la libertad de las personas proveniente de un uso ilegítimo del tratamiento de datos. Dentro del concepto de dato se comprende también a los datos personales públicos, datos que por el hecho de ser accesibles al conocimiento de cualquiera no escapan tampoco al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. Igualmente, se debe señalar que dentro de los datos amparados por este Derecho no sólo encuentran protección los relativos a la vida privada o íntima de la persona, sino también, todos aquellos que identifican o permiten identificar a la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole o, para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo. Es importante apuntar que en este derecho, todos los datos personales pertenecen a la persona, titular de los mismos y, su apropiación por otro sujetos no titular del dato sólo es posible si cuenta con el consentimiento de la persona, salvo que una norma con rango de Ley establezca lo contrario.

En conclusión, el concepto de dato es muy amplio y comprende a todos los datos que se refieren a las personas, en nuestro caso a las personas mayores, incluidos aquellos que recogen la imagen. De ahí que todo tratamiento de datos de las

personas mayores que se desarrolle debe, necesariamente, respetar lo dispuesto en la LOPD y normativa de desarrollo.

3.2. El tratamiento de los datos, el consentimiento y otros aspectos relevantes

Los datos personales para ser objeto de protección por la LOPD deben ser sometidos a tratamiento, es decir, deben ser incluidos en un fichero, considerado por la propia norma (artículo 3.b).), como "*conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*". El fichero que así se vaya a constituir, se encuentra sometido a la LOPD y, consecuentemente, es obligatoria su inscripción en el Registro General de Protección de Datos correspondiente por parte del responsable del fichero, previo a la introducción en el mismo de cualquier dato[8]. De ahí que todos los ficheros en los que se vayan a incluir datos de las personas mayores se encuentran sujetos a esta normativa, normativa que contiene diferente procedimiento de inscripción según se trate de ficheros públicos o de ficheros privados[9]. En efecto, si se trata de un fichero cuya titularidad es pública -por ejemplo los ficheros de los Servicios Sociales de la Administración Pública, sea Estatal, Autonómica o Local-, la creación de los mismos se debe realizar mediante disposición de carácter general[10]. Si, por el contrario, se trata de un fichero privado –datos que puede tener un centro asistencial privado-, se debe notificar a la Agencia Española de Protección de Datos (única competente para inscribir y controlar este tipo de ficheros) por medio de unos modelos normalizados que la propia Agencia dispone y en las que se debe indicar el tipo de fichero, el responsable del fichero, la finalidad del mismo, 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 piensan realizar y, en su caso, las transferencias de datos que se prevean efectuar a países terceros. Ambos tipos de ficheros, públicos o privados, se deben inscribir obligatoriamente en el Registro General de Protección de Datos correspondiente, Registro cuya consulta es pública. En consecuencia, la notificación de los ficheros siempre debe ser previa a la introducción en los mismos de datos y, la ausencia de

[8] El artículo 26 de la LOPD, titulado Notificación e inscripción registral dispone que: *"Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, 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. Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá 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 Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos."*

[9] De acuerdo con aquella diferencia el RLOPD establece que:

Son **Ficheros de Titularidad Pública** *"los ficheros de los que sean responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a los mismos, las Administraciones Públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público"* (artículo 5.1 m) RLOPD)

Son **Ficheros de Titularidad Privada**, *"los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las Corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica"* (Artículo 5.1 l) RLOPD)

[10] La Agencia de Protección de Datos de la Comunidad de Madrid contiene dicha previsión en el artículo 20 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal; artículo desarrollado por Decreto 99/2002, de 13 de junio, de Regulación del Procedimiento de Elaboración de Disposiciones de Carácter general de Creación, Modificación y Supresión de Ficheros que contienen Datos de Carácter Personal, así como su inscripción en el Registro de Ficheros de Datos Personales.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

dicha notificación e inscripción, es constitutiva de una infracción leve con arreglo a lo dispuesto en el artículo 44.2.c) de la propia Ley, infracción que será sancionada con multa de 900 a 40.000 euros –art. 45-1-.

El fichero con los datos debe cumplir a lo largo de su existencia con los principios de protección de datos recogidos en la LOPD. En efecto, la citada norma legal concreta los requisitos de calidad de los datos –art. 4), el derecho de información en la recogida de los mismos (art. 5), la obligación de contar con el consentimiento del titular de los datos (art. 6), el principio de datos especialmente protegidos (art. 7), la seguridad de los datos (art. 9), el deber de secreto (art. 10), la comunicación de los datos (art. 11) y el acceso a los mismos por cuenta de terceros (art. 12). El omitir aquellos principios puede constituir infracciones graves o muy graves sancionadas con multa que oscilan entre los 40.001 a 600.000 euros.

Un aspecto esencial en materia de protección de datos es el consentimiento del titular del dato que exige la LOPD y su normativa de desarrollo. Dicho consentimiento otorgado en nuestro caso, por la persona mayor o por su representante legal, es definido por la LOPD (y en igual sentido en el Reglamento) como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"* -art. 3.h)-. De acuerdo condicha definición el consentimiento debe reunir las siguientes características:

a) **Manifestación voluntaria**: es decir, que exprese que se está conforme con el fin para el que se trata el dato
b) **Libre**, que el consentimiento se obtenga sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.
c) **Inequívoca**: que no exista duda alguna sobre la prestación de dicho consentimiento, que aparezca como evidente[11].
d) **Específica,** referido a una determinada operación de tratamiento y para una finalidad concreta, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.
e) **Informada**: el consentimiento, además de previo, específico e inequívoco, deberá ser informado. Esta información debe ser plena y exacta acerca del tipo de tratamiento y su finalidad, con advertencia sobre el derecho a denegar o retirar el consentimiento. La información así configurada debe tomarse como un presupuesto necesario para otorgar validez a la manifestación de voluntad del afectado (art. 5 LOPD)

En consecuencia, todo tratamiento de datos sin consentimiento del titular del dato constituye un límite al Derecho fundamental a la Protección de Datos, derecho fundamental, en palabras del Tribunal Constitucional que "...*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un* particular*, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de*

[11] La Sentencia de la Audiencia Nacional, de 21 de noviembre de 2007, concreta al respecto que el legislador al utilizar este término acudió a un criterio sustantivo, es decir, indicativo de que cualquiera que sea la forma que revista el consentimiento éste ha de aparecer como evidente, es decir, que no admite duda o equivocación. Es por tanto, éste y no otro, el significado del adjetivo utilizado –inequívoco- para calificar al consentimiento. Por ello, cuando existan presunciones o alusiones a la publicidad de sus datos en otro lugar, resulta, a todas luces, irrelevante, pues dar carta de naturaleza a este tipo de interpretaciones pulverizaría esta exigencia esencial del consentimiento, porque dejaría de ser inequívoco para ser "equivoco", es decir, su interpretación admitiría varios sentidos y, por esta vía, se desvirtuaría la naturaleza y significado que desempeña como garantía en la protección de los datos, e incumpliría la finalidad que está llamado a verificar, esto es, que el poder de disposición de los datos corresponde únicamente a su titular.

datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"[12].

Son pues elementos característicos del Derecho Fundamental a la Protección de Datos Personales, los derechos del afectado a consentir informadamente sobre la recogida y el tratamiento de sus datos personales y a saber el destino de los mismos. La información se convierte en una pieza clave del consentimiento y se concreta en el artículo 5 LOPD, que dispone:

> "1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
>
> a) 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.
>
> 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.
>
> e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
>
> Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
>
> 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
>
> 3. No será necesaria la información a que se refieren las letras b, c y d del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
>
> 4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá 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 lo previsto en las letras a, d y e del apartado 1 del presente artículo.
>
> 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
>
> Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando 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 informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".

[12] Sentencia 292/2000, de 30 de noviembre, F.J. 7 primer párrafo.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

Ahora bien, en derecho y con carácter general, el consentimiento se puede otorgar de distintas formas[13]:

a) **Expreso**, manifestado mediante un acto positivo y declarativo de la voluntad
b) **Tácito**, cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume o se presupone como un acto de aquiescencia o aceptación.
c) **Presunto**, que no se deduce ni de una declaración ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación.

A efectos de lo dispuesto en la LOPD, tan sólo son aceptables los dos primeros modos de prestar el consentimiento, es decir, el expreso y el tácito, no admitiéndose bajo ningún punto de vista el consentimiento presunto.

Igualmente, es preciso indicar que los datos de carácter personal que sean objeto de tratamiento sólo pueden ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y siempre que exista previo consentimiento del interesado. Este procedimiento se conoce como "cesión de datos", cesión que será nula si la información que se facilita por el titular del dato no le permite conocer la finalidad a que se destinan los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. En todo caso, tal como establece la LOPD, aquel a quien se comunican los datos de carácter personal, cesionario, se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la LOPD.

De conformidad con lo expuesto *ut supra* y, de acuerdo con las numerosas resoluciones de las Agencias de Protección de Datos – Estatal y autonómicas-, es necesario que el responsable del tratamiento de los datos cuente con el consentimiento para el tratamiento de dichos datos personales, entendido este último –art. 3 de la LOPD- como: ***Responsable del fichero o tratamiento****: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento."*

En consecuencia, todos los tratamientos de los datos de las personas, también el de las personas mayores, precisan haber obtenido el consentimiento del interesado o, en su caso, contar con la autorización de una norma con rango de Ley que permita su recopilación. El artículo 6 de la LOPD contiene otros supuestos -apartado 2- muy importantes de dispensa de la obtención del consentimiento cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias
b) Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento
c) Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley
d) Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea 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.

[13] Véase en este sentido las numerosas Sentencias del Tribunal Supremo que al respecto existen, entre las que cabe destacar, las STSs de 26 de mayo de 1.986 o la de 11 de junio de 1.991que interpretan el artículo 1.253 del Código Civil.

Al responsable del fichero es a quien le corresponde acreditar que el consentimiento fue otorgado por el titular del dato con pleno cumplimiento de los requisitos antes expuestos . En efecto, el artículo 12 del RLOPD, recoge aquella exigencia de manera expresa señala que *"corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho*.". La propia Agencia Española de Protección de Datos destacó al respecto que, si bien es cierto que el artículo 6 de la LOPD no señala la obligación de guardar prueba documental, se ha entendido que cualquier medio valido en derecho, conjugado con circunstancias concurrentes, sirven para acreditar el consentimiento (sin perjuicio de que para ciertos datos personales, éste haya de ser expreso)[14]. El no poder demostrar por el responsable que se cuenta con el consentimiento del afectado puede llevar aparejada una sanción considerada grave y tipificada en el artículo 44.3.c) de la LOPD, que dispone: "…*Son infracciones graves:….c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave";* infracción que, de acuerdo con lo establecido en el artículo 45.2 de la LOPD, será sancionada con multa de *40.001 a 300.000 euros.*

Con carácter general, las sanciones que la AEPD imponga puede ser graduada atendiendo a determinadas circunstancias que permiten modular o adecuar la imposición de la sanción a la trascendencia de la infracción y hechos cometidos. De acuerdo con el artículo 45, que sistematiza los criterios de graduación, se deberá valorar la naturaleza de los derechos afectados, el volumen de los tratamientos efectuados, los beneficios obtenidos, el grado de intencionalidad, la reincidencia, los daños y prejuicios causados, la antijuridicidad de los hechos o a la culpabilidad del afectado, entre otras causas[15].

Igualmente, después de la reforma introducida por la Ley 2/2011, de 4 de marzo, de economía sostenible, la Agencia de Protección de Datos correspondiente, podrá acordar la no apertura del procedimiento sancionador, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios antes señalados y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las

[14]Recordemos que el citado precepto dispone "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa."*.

[15] El artículo 45.*4 LOPD*, dispone *"La cuantía de las sanciones se graduará atendiendo a los siguientes criterios: El carácter continuado de la infracción.*
El volumen de los tratamientos efectuados.
La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
El volumen de negocio o actividad del infractor.
Los beneficios obtenidos como consecuencia de la comisión de la infracción.
El grado de intencionalidad.
La reincidencia por comisión de infracciones de la misma naturaleza.
La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
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 Ios 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.
Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. El órgano sancionador establecerá 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, en los siguientes supuestos:
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 el apartado 4 de este artículo.
Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
Cuando el infractor haya reconocido espontáneamente su culpabilidad.
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.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

medidas correctoras que en cada caso resulten pertinentes; excepción que sólo se puede aplicar siempre que no se trate de un hecho muy grave y que el infractor no hubiese sido sancionado o apercibido con anterioridad –art. 45.6-.Si el apercibimiento no fuera atendido por el infractor en el plazo que el órgano sancionador hubiera determinado se procederá a la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

En conclusión, para poder usar los datos de las personas mayores, bien sea por parte de los poderes públicos como por los propios sujetos privados, es preciso contar siempre con el consentimiento del titular del dato, salvo que una Ley lo permita o se encuentre incurso en alguno de los supuestos previstos en el artículo 6.2 de la LOPD. De ahí que todas aquellas personas que acompañan, ayudan o asisten a las personas mayores no pueden válidamente dar el consentimiento para el tratamiento de datos de las citadas personas, dado que sólo el titular del dato es el que puede válidamente otorgar el consentimiento. Corresponde al propio responsable demostrar, como hemos visto, el otorgamiento del consentimiento por el titular del dato sin que sea válido el otorgado por otro sujeto, salvo que dichas personas se encuentren autorizadas por Ley o se trate de sus representantes legales.

3.3. Los datos especialmente protegidos

Existen una serie de datos de carácter personal que cuentan con una protección especial singularmente reforzada dado que forman parte de la esfera más íntima de las personas. Estos datos, denominados por la LOPD "datos especialmente protegidos", se regulan en el artículo 7 de la citada ley. Se consideran dentro de esta clasificación:

a) Los datos relativos a *ideología, religión, afiliación sindical o creencias*. En este caso, nadie puede ser obligado a declarar estos datos y el consentimiento debe ser otorgado de forma expresa y por escrito, con advertencia de su derecho a no prestarlo. Se exceptúa de esta regulación, los ficheros mantenidos por los 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, sin perjuicio de que la cesión de dichos datos precise siempre el previo consentimiento del afectado.
b) Los datos de carácter personal que hagan referencia al *origen racial, a la salud y a la vida sexual*. En este supuesto los datos sólo pueden ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

En relación con estos dos grupos de datos, la LOPD contiene unas prohibiciones comunes tales como crear ficheros que contengan este tipo de dato cuando la finalidad sea exclusivamente almacenarlos. La propia LOPD permite el tratamiento de ambos tipos de datos cuando resulte 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 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 la Ley autoriza el tratamiento de ambos grupos de datos cuando 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.

c) Los datos de carácter personal relativos a la *comisión de infracciones penales o administrativas*. Estos datos sólo pueden ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

En consecuencia, los datos relativos a *ideología, religión, afiliación sindical o creencias, salud, origen racial o vida sexual* cuentan con un tratamiento especial, de tal forma que nadie está obligado a facilitar dichos datos, salvo que una Ley habilite al efecto. En este sentido, corresponde destacar que el cumplimiento de todos estos requisitos en el caso de las personas mayores resulta complicado, dado que en los supuestos en los que las personas mayores se encuentren en situación de Dependencia, todas aquellas personas que las acompañan o asisten, salvo que se trate de sus representantes legales, no pueden ceder los datos de las personas que asisten o acompañan a terceros, salvo que una ley lo permita. Corresponde a los responsables del tratamiento verificar que existe un consentimiento claro, preciso, inequívoco e informado de la persona titular del dato. El cumplimiento de estas exigencias no siempre resulta fácil porque los mayores no se encuentran en condiciones de otorgar aquel tipo de consentimiento y además no cuentan con un representante legal.

3.4. Los datos registrados en soporte físico

Finalmente, cabe destacar que el régimen jurídico de la protección de datos se extiende a los datos de carácter personal que estén registrados en un soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de los datos por los sectores público y privado –art. 2. 1 LOPD-. Esta previsión es trasposición del artículo 3 de la Directiva 95/46 CE, de 24 de octubre de 1995 antes citada que señala que *"sus disposiciones se aplicarán al tratamiento total o parcialmente automatizado de datos de carácter personal, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."*. Por su parte el RLOPD, define a los Fichero no automatizado como *"todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"* y somete los mismos a la adopción de unas medidas de seguridad importantes recogidas en el Título VIII, Capítulo IV del citado reglamento. De ahí que, todos los ficheros que incorporen datos de carácter personal y se encuentre en soporte papel debe cumplir con los mandatos de la LOPD, en especial con los principios de protección de datos y los derechos de las personas.

4. El tratamiento de los datos personales en algunos ámbitos que afecta a las personas mayores

4.1. Utilización de los datos personales de las personas mayores por los centros asistenciales

4.1.1. Planteamiento de la cuestión

Muchas personas mayores, en especial aquellas que se encuentran en situación de dependencia, es posible que estén relacionadas con un centro asistencial (bien de día, de noche o todo el tiempo). Este centro, lógicamente, para el desarrollo de su actividad, precisa recoger y tratar los datos de las personas mayores con las que se relaciona, tales como datos identificativos, datos especialmente protegidos –como los datos de salud-, datos relacionados con circunstancias personales, datos familiares, etc.. Los citados datos, serán objeto de tratamiento e incorporados a la denominada Historia Social del paciente y, al igual que cualquier otro dato, el centro que los recoja debe, en todo caso, respetar lo establecido por la LOPDC[16]. De ahí el estudio de esta materia.

[16] Para el desarrollo de este punto, se ha tenido en cuenta, fundamentalmente, las distintas Recomendaciones que la Agencia de Protección de Datos Comunidad de Madrid ha elaborado. Se trata de la Recomendación 1/2005, de 5 de agosto, sobre el Archivo, Uso y Custodia de la Documentación que compone la Historia Social por parte de los Centros Públicos de Servicios Sociales de la Comunidad de

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

4.1.2. La Historia Social, definición

Normalmente, los datos de carácter personal que se recogen de las personas mayores en un centro asistencial serán incorporados a la denominada "Historia Social". Esta es definida, como un instrumento documental en el que se registran exhaustivamente los datos personales, familiares, sanitarios, de vivienda, económicos, laborales, educativos y cualquier otro significativo de la situación socio-familiar del usuario, así como la demanda, el diagnóstico y la subsiguiente intervención en la evolución de su situación personal[17]. La historia social puede estar en soporte papel (fichero no automatizado) o en soporte informático (fichero automatizado), siendo siempre recomendable este último.

La citada historia social permite a los trabajadores sociales analizar, sintetizar, describir y cuantificar las situaciones de las personas mayores que se benefician de los servicios sociales. La valoración que los trabajadores sociales obtienen de los datos contenidos en la historia, les permite obtener un punto de vista personal del paciente y, además, conocer determinadas características del entorno en el que la persona mayor desarrolla su vida. De ahí la importancia de la historia social, dado que el trabajador social habilitado, es decir aquel responsable de valorar a la persona mayor –no cualquier trabajador social–, puede acceder a los datos que son necesarios para ofrecer una asistencia social adecuada, fijar los objetivos que debe cumplir y establecer un plan de trabajo, con calendarios y con períodos y procedimientos de intervención.

Ahora bien, es preciso indicar que los trabajadores sociales –y todos aquellos que estén autorizados para trabajar con la historia social- sólo podrán consultar de la citada historia, única y exclusivamente, aquellos datos que sean estrictamente necesarios para la gestión del servicio social que se presta. De ahí, que los datos que se recojan deban ser adecuados y pertinentes y no excesivos para la gestión y siempre se debe proceder a la cancelación de los mismos.

4.1.3. Los datos personales de las personas mayores y su inclusión en las historias sociales

Todos los datos personales pertenecientes a las personas mayores y el tratamiento de los mismos contenidos en la historia social se deben ceñir a aquellos que sean estrictamente necesarios para la gestión del servicio social prestado. Si, en algún momento se hubiese recabado algún dato que, con posterioridad, se verifique que no es adecuado o pertinente o excesivo para la gestión que se desarrolla, el centro asistencial como Responsable debe proceder, de forma inmediata y de oficio a la cancelación o al borrado de los mismos. La valoración relativa sobre estas cuestiones corresponde al responsable del fichero del centro que, como hemos visto, es quien debe garantizar el cumplimiento de la LOPD y, en especial, la calidad de los datos contenidos en el fichero, en nuestro caso de la historia social, dada la heterogeneidad de datos que puede tener el mismo en función del servicio que

Madrid y la Recomendación 1/2008, de 14 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el Tratamiento de datos personales en los Servicios Sociales de la Administración de la Comunidad de Madrid y en los Servicios Sociales de los Entes locales de la Comunidad. En las citadas Recomendaciones se definen aspectos tan importantes como la Historia Social, su contenido y los distintos usos que se pueda realizar de la misma, o los distintas competencias que tienen asignados los Servicios Sociales y, en consecuencia, los datos que pueden recabar. En este sentido, si bien las Recomendaciones se limitan al ámbito de los centros asistenciales públicos autonómicos y locales, es también extensible para el resto de centros que cuidan a personas mayores. De ahí su estudio. Finalmente, también interesa destacar, el estudio del Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA), inscrito en el Registro de la Agencia Española de Protección de Datos, con fecha 27 de diciembre de 2004, en donde se contiene una importante consideración sobre la actuación que los distintos centros asistenciales deben tener presente a la hora de realizar su función. Finalmente, mencionar, el Dictamen de la Agencia de Protección de Datos Vasca de 2009, emitido en relación con el servicio de teleasistencia.

[17] Recomendación 1/2005, de 5 de agosto, sobre el Archivo, Uso y Custodia de la Documentación que compone la Historia Social por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid.

preste. En definitiva, el responsable es quien debe decidir sobre la finalidad, contenido y uso del tratamiento, por lo que en principio, la responsabilidad del archivo y gestión del fichero será de éste. Normalmente, dicha figura en los centros que prestan servicios sociales suele ser asumida por la Dirección del mismo, salvo que se encomiende a una unidad, departamento o servicio específico dentro de cada uno de ellos.

En cualquier caso, es importante destacar que el citado centro, previo a la recogida de cualquier dato, debe haber procedido al registro del fichero correspondiente en la Agencia de Protección de datos que corresponda -Agencia Autonómica, en el caso de tratarse de ficheros públicos o en defecto de éstas, en la Agencia Española de Protección de Datos o, si se trata de ficheros privados, en la Agencia Española de Protección de Datos. Recordemos, que de acuerdo con el artículo 44.3 a) de la LOPD, se considera infracciones graves "*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*"; infracción que, de acuerdo con lo establecido en el artículo 45.2 de la misma ley serán sancionadas con multa de 40.001 a 300.000 euros. Sin embargo, es constitutivo de una infracción leve la ausencia de inscripción de un fichero privado.

Con carácter general, la Historia social de las personas mayores puede contener, los siguientes tipos de datos:

a) Los datos relativos a la identificación del residente o usuario
b) Los datos relativos de sus familiares
c) Las prescripciones médico-farmacéuticas

Corresponde al usuario o residente del servicio o, en su caso, a su representante, facilitar todos aquellos datos relevantes que dispongan de forma leal y verdadera para la prestación de la asistencia. Igualmente, los trabajadores sociales, deben reflejar en la citada historia cualquier dato que consideren relevante en tanto que permita conocer la situación personal del demandante o usuario de un servicio social.

4.1.4. El caso peculiar de los datos relativos a la religión de las personas mayores

Como hemos visto, el dato religioso es un "dato especialmente protegido", lo que supone que cuenta con un régimen especial. En algunas ocasiones, puede ocurrir, que los centros asistenciales precisen tratar datos relativos a la religión del residente o usuario para ofrecer una correcta y adecuada prestación del servicio a la persona mayor. Así por ejemplo, el tratamiento del dato religioso por parte del centro puede estar justificado en la necesidad de conocer la voluntad de la persona de asistir o no a determinados oficios religiosos que se celebren en el centro, como por ejemplo, ir a misa. En otros, puede ser que el centro tenga que saber los alimentos que la persona mayor quiere comer y aquellos que no se pueden dar por estar prohibidos por su religión o creencias. También puede ocurrir que el deseo de la persona mayor sea el de recibir o no, determinados tipos de tratamientos médicos como no recibir transfusiones de sangre por no permitírselo su religión o creencias.

En todos estos casos es, al Responsable del fichero, a quien corresponde valorar, de acuerdo con el principio de proporcionalidad, los datos que se deben recoger y en qué forma. Es decir, de acuerdo con el citado principio, seguramente no es necesario recoger en la historia social, los datos relativos a la religión de la persona si la finalidad se consigue con una relación en la historia social de los alimentos que la persona no debe comer. En otro caso, seguramente, sea preciso recogerlos, como la asistencia a determinado rito religioso de la persona. Igualmente, puede

ocurrir que este tipo de datos -relativos a la religión- lleguen al centro a través de los informes sociales elaborados por los trabajadores sociales ajenos al centro.

En todos estos supuestos, si el centro decide incluir este tipo de datos en la historia, como l Responsable del fichero debe solicitar el consentimiento expreso y por escrito del titular del dato o su representante legal para poder incorporarlo al expediente asistencial. En caso contrario, no es posible incorporar los mismos y se debe proceder a eliminarlos Recordemos que la LOPD considera infracción muy grave -artículo 44.3.a)-, recabar y tratar datos de carácter personal mencionados en el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; infracción que, de acuerdo con lo establecido en el artículo 45.3 de la LOPD, será sancionadas con multa de 300.001 a 600.000 euros.

4.1.5. Documentos que integran la Historia Social

Todos los datos que tenga el Centro relativos a la persona se deben integrar en la historia social que se compone de varios documentos, tales como la ficha social, el informe social y todos aquellos otros que recojan las intervenciones realizadas y las informaciones que avalen los datos contenidos en la historia.

Los datos personales que en la historia se recaban, pueden ser gestionados bien a través de archivos en soporte papel, bien a través de archivos en soportes informáticos. Es decir, los tratamientos de datos personales como hemos visto, pueden ser automatizados o no automatizados (art. 3.c) LOPD). Aunque el régimen jurídico de los ficheros informatizados y manuales es parcialmente distinto, baste destacar que ambos tipos de ficheros les es plenamente aplicable los principios de la protección de datos (arts. 4 a 12 LOPD) y los derechos de las personas que en este ámbito tienen reconocidos (art. 13 a 19 LOPD).

Como se apuntó anteriormente, la historia social se compone de los siguientes documentos[18]:

a) Ficha Social: donde se registra la información sistematizable, y aunque no existe un modelo normalizado suelen recogerse los datos del usuario, de su entorno socio-familiar, de su medio y de la intervención social.
b) Proyecto de intervención social: que contiene el diseño de la intervención social, comprensiva de la evaluación, el diagnóstico de la situación y la determinación de objetivos operativos, actividades, tareas, recursos, calendarios y criterios de valoración.
c) El informe social: que comprende la valoración realizada por un profesional social como resultado de un proceso y en el que se concretan, los hechos, la valoración y las recomendaciones que se formulan por el citado profesional.
d) Todos aquellos otros documentos donde se reflejen el seguimiento de las intervenciones que se realicen o los que avalan y aportan la información contenida en la historia social.

No se consideran comprendidos dentro de la historia social todos aquellos documentos que se tramiten por los Servicios competentes y que tengan como finalidad reconocer o dar determinadas prestaciones sociales, como una subvención, o una situación legal o de hecho o la concesión de una prestación específica. Sin embargo, es preciso indicar, que el hecho de que no se integren los citados documentos en la historia social, no significa que no estén sujetas a la LOPD.

[18] Recomendación 1/2005, de 5 de agosto, sobre el Archivo, Uso y Custodia de la Documentación que compone la Historia Social por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid y la Recomendación 1/2008, de 14 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el Tratamiento de datos personales en los Servicios Sociales de la Administración de la Comunidad de Madrid y en los Servicios Sociales de los Entes locales de la Comunidad.

4.1.6. Los Derechos, la información y el consentimiento de las personas mayores

Corresponde a los centros asistenciales, en especial al responsable del fichero, facilitar el ejercicio de los derechos reconocidos por la normativa de protección de datos a los residentes o usuarios así como cumplir con las obligaciones de adaptación al marco legal de protección de datos de carácter personal y, en especial, la obligación de información en la recogida de los datos así como guardar la máxima confidencialidad en todo lo referente a la privacidad de los datos de las personas mayores de edad. En este sentido, es preciso destacar que cuando se recaban datos personales para ser incorporados a la historia se deba informar a los usuarios, en la recogida, sobre la existencia del fichero, la finalidad y los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta, de las consecuencias de la obtención de los datos y de la negativa a suministrarlos. Igualmente, es preciso indicar, la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición así como la identidad y dirección del responsable del fichero para hacer efectivo los derechos que le reconoce la legislación. Como regla general, dicha recogida e información se suele facilitar por medio de formularios o impresos o a través de entrevista personal o también a través de medios telemáticos. En cualquiera de ellos se debe ofrecer siempre la información antes señalada (art. 5 LOPD).

Es importante destacar, en especial con la dación de información y el consentimiento del titular de los datos que, en el caso de las personas mayores, pueden darse distintas situaciones que es preciso valorar:

1. En primer lugar, cuando la persona mayor tiene plena capacidad. En este caso puede expresar libremente su voluntad, de acuerdo con lo dispuesto en el Código Civil y por ello, el ejercicio de los derechos que la LOPD les reconoce pueden ser ejercitados directamente por la persona.
2. En segundo lugar, puede ocurrir que la persona mayor haya sido declarada incapaz por una sentencia judicial firme. En este caso, debe actuar representado por la persona designada como su tutor en la sentencia judicial de incapacitación.

No obstante, los dos supuestos anteriores, también puede ocurrir que la persona mayor no haya sido declarado incapaz por sentencia firme pero la misma padece algún tipo de demencia o deterioro cognitivo que le impide manifestar su voluntad libremente. En este caso, se debe diferenciar si la persona tiene un representante legal o no. Si la persona mayor cuenta con representante legal, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición pueden ser ejercidos por éste sin ningún problema. En cambio si no existe un representante legal, la situación se complica dado que en principio y hasta tanto no exista una declaración jurídica al respecto, la persona se considera capaz a todos los efectos. En alguna ocasión no obstante, se acepta que se acredite la existencia de un representante voluntario que haya sido expresamente designado para el ejercicio del derecho y siempre que conste claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél[19].

Teniendo en cuenta lo anterior, el tratamiento de los datos de las personas mayores y la correspondiente incorporación de los mismos a un fichero requiere, con carácter general, el consentimiento del interesado, salvo que una Ley disponga otra cosa. No será necesario el consentimiento, entre otros, como hemos visto, cuando el centro sea público y los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias o,

[19] Véase en este sentido, el Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA), inscrito en el Registro de la Agencia Española de Protección de Datos, con fecha 27 de diciembre de 2004.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento (art. 6.2 LOPD). Recordemos, en este sentido, que si se trata de un centro o institución privada existe normalmente un contrato con el residente o usuario del servicio.

En todo caso, con carácter previo a la recogida se debe informar al usuario o a la persona que lo represente legalmente, de forma precisa, inequívoca y entendible por el receptor de la información de los términos que establece el artículo 5 de la LOPD y que vimos anteriormente. Tan sólo indicar que se ha considerado cumplido el deber de información cuando se presta a través de carteles informativos siempre que los datos no se recojan en formularios. Igualmente, es obligado para los centros articular sistemas que permitan facilitar la información del artículo 5 LOPD cuando los datos se recaban a través de teléfono, Internet o mensajes SMS.

Es importante señalar los principios que rigen el tratamiento de datos personales, recogido en el artículo 4.1 de la LOPD que, recordemos, consagra que "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*" De ello se desprende la necesidad de que el tratamiento de un determinado dato de carácter personal deba ser proporcionado a la finalidad que lo motiva. De ahí que el centro asistencial sólo podrá recoger los datos necesarios para la prestación de los servicios asistenciales, que incluye la información relativa a la salud del residente o usuario necesaria para darle la prestación, y otros datos destinados a la administración de esos servicios y a la relación jurídico-contractual existente entre el centro o establecimiento asistencial y el residente o usuario.

No se puede olvidar que esta información constituye la herramienta, básica y fundamental, que permite al centro realizar las tareas que tiene encomendadas para prestar asistencia a quienes la necesiten o demanden, permitiéndole analizar, sintetizar, cuantificar y describir las situaciones de los usuarios tanto a nivel personal como en relación a su entorno. Para cumplir con esta finalidad y, siempre que se cuente con el consentimiento expreso del usuario o de su representante legal, sería posible recoger en el citado expediente, aquellos datos de salud que reflejen situaciones de incapacidad o minusvalía, física o psíquica, reconocida legalmente o de hecho, o cualquier otro dato de salud que pueda afectar y repercutir en la situación personal y social del usuario o beneficiario de la prestación social.

Igualmente, es preciso destacar que los centros sólo deben utilizar los datos que se encuentran en sus ficheros, para las finalidades legítimas y nunca para una finalidad incompatible con la que motivó su recogida. Se considera compatible cuando se utiliza posteriormente esos datos con fines históricos, estadísticos y científicos y cuando ese uso posterior se realice de forma disociada[20]. Por el contrario, se considera incompatible, cuando el uso de la información contenida en la historia social se utiliza para el envío de difusión de mensajes de contenido político.

4.1.7. La conservación de los datos que se encuentran insertos en las historias sociales

La conservación de las historias sociales, sean manuales o informáticas y, por tanto, de los datos personales que éstas contienen, no puede ser indefinida. Para ello, es preciso tener en cuenta si la historia social se encuentra en situación "activa" o, por el contrario, "pasiva". En el primer caso, se considera que la Historia social está activa cuando la misma tiene utilidad para la prestación social al

[20] Recordemos que un dato disociado es aquél que no permite la identificación de un afectado o interesado (art. 5 e) RDLOPD.

usuario. Por el contrario, se encontrará en situación de pasiva cuando la historia social no sea necesaria para la prestación correspondiente. En el supuesto que esté activa los datos personales se deben conservar durante el tiempo que se presta asistencia social y, además, durante un mínimo de tiempo desde que dicha asistencia social finalice en tanto que se considere que puede ser útil para posibles nuevas actuaciones. La consideración de la utilidad o no de la historia y, por tanto, del tiempo que debe conservarse los datos, no se encuentra establecido en norma alguna. Sin embargo, las Agencia de Protección de Datos de la Comunidad de Madrid ha considerado que se corresponde la aplicación analógica del plazo contemplado para conservar la historia clínica, de cinco años como mínimo desde que ha finalizado la prestación social correspondiente –plazo contenido en 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-. Una vez transcurrido dicho plazo, se debe considerar que la historia social pierde su utilidad y, consecuentemente, se convierte en "pasiva", en cuyo caso sólo se debe mantener los datos a efectos judiciales y, el centro debe remitir la historia social para su conservación al archivo central correspondiente.

Finalmente corresponde destacar que una vez cumplido el período antes señalado, los datos personales sólo se podrán conservar si se someten a un proceso de disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la LOPD, y en el RLOPD.

4.1.8. Acceso a los datos contenidos en la historia social de una persona mayor por parte de terceros

El acceso a la información o a los datos personales que la historia social contiene no puede estar abierto a todas aquellas personas que lo soliciten, sean éstos empleados, familiares, amigos, médicos, etc. Por el contrario, la LOPD y su desarrollo reglamentario, exigen al Responsable del fichero que adopte las medidas necesarias para limitar el acceso sólo a aquellos sujetos que por su actividad o interés deban acceder a la historia. Con esta finalidad, el Responsable del fichero debe articular distintos sistemas por medio de los cuales garantice que el acceso a los datos contenidos en la historia social sólo pueda efectuarse por aquellas personas que se encuentren legitimadas por las funciones que desarrollan. Para ello, es preciso definir los perfiles de acceso de cada empleado o trabajador según las funciones que tengan encomendadas, concretando en cada supuesto a qué datos pueden acceder en cada caso. A título de ejemplo, es posible indicar, algunos accesos que es posible autorizar:

a) En principio, el acceso a la historia social de un usuario sólo se puede permitir a aquellos profesionales que participan en el proceso asistencial y, siempre que el acceso, sea necesario para el ejercicio de sus funciones.
b) Igualmente, también se puede permitir el acceso a la historia social para la realización de tareas de planificación y programación de servicios del centro, siempre que, en este caso, se preserven los datos que identifican al titular de los datos de carácter personal que se encuentren en la historia.
c) Por otra parte, también los responsables de los centros públicos o de las unidades u órganos administrativos de que éstos dependan, o en su caso, de los centros privados, podrán acceder a las citados expedientes de los usuarios para, del análisis del conjunto de las mismas, tener una visión global de lo que sucede en la realidad social en que estén actuando, información que les permitirá optimizar los recursos y mejorar la calidad de los mismos. El acceso en este caso a los datos con la finalidad antes indicada obliga, con carácter previo al acceso a la información que vaya a ser objeto de análisis, a preservar en todo caso los datos que identifican al titular de los datos de carácter personal que consten en las mismas.

d) La realización de tareas de gestión de los servicios y administrativas también habilita para acceder a la información almacenada en el expediente de los usuarios. En este caso el acceso estará limitado a aquellos datos que sean adecuados, pertinentes y no excesivos para la gestión o tarea concreta que se deba realizar, como por ejemplo la admisión del usuario en el centro; funciones de gestión, contables o presupuestarias, etcétera.
e) En otros supuestos, también puede ocurrir que el acceso a dicha información, se encuentre amparada por lo dispuesto en el artículo 6.2 de la LOPD, en tanto que existe una relación contractual.

En todos estos casos, todas las personas que accedan a los datos están sujetas al deber de secreto recogido en el artículo 10 LOPD, que obliga tanto a los responsables como a todos los que intervengan en cualquier fase del tratamiento de los datos de carácter personal al secreto profesional y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. Paral ello, se considera importante que todas las personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal suscriban el "Compromiso por escrito de guardar secreto sobre los mismos"[21]. Igualmente, es preciso indicar que dependiendo del nivel de seguridad que el fichero tenga, será necesario que el acceso a los datos quede registrado, dado que el acceso sin estar legitimado para ello, puede constituir una infracción grave o muy grave de acuerdo con la LOPD (art. 44).

4.1.9. La prestación de asistencia social y sanitaria a las personas mayores en el centro. Necesidad de contar con historia social e historia clínica

En algunos centros, además de la asistencia social que se les da a las personas mayores, también es posible que se les ofrezca asistencia sanitaria. En este caso, los sujetos que presten ambas asistencias serán distintos. En el primer caso, será el trabajador social y, en el segundo, los profesionales sanitarios. En estos casos, corresponde también al Responsable del fichero diferenciar y separar el archivo y custodia de los datos que componen la historia social de aquellos que tienen un fin específicamente asistencial sanitario y que se integran en la historia clínica del usuario. Como luego tendremos ocasión de estudiar, la historia clínica cuenta con una regulación propia recogida en 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 y en la normativa autonómica existente.

Cuando se ofrecen las dos prestaciones, los centros asistenciales deben organizar sus expedientes separándolos, uno de carácter asistencial y otro de historial clínico debidamente diferenciados. No obstante, es preciso indicar que, si se cuenta con el consentimiento expreso del usuario o de su representante legal, es posible recoger en la historia social, aquellos datos de salud que reflejen situaciones de incapacidad o minusvalía, física o psíquica, reconocida legalmente o de hecho, o cualquier otro dato de salud que pueda afectar y repercutir en la situación personal y social del usuario o beneficiario de la prestación social.

En cuanto al historial clínico cabe destacar que únicamente puede ser consultado por el médico responsable, sin perjuicio de lo dispuesto en la normativa estatal y autonómica en materia de inspección de salud y servicios sociales. Por los mismos motivos, los profesionales que presten asistencia sanitaria a los usuarios no pueden sin más acceder a los datos contenidos en el expediente asistencial, datos a los que sólo podrán acceder cuando tengan una relación directa con el posible diagnóstico o tratamiento de la salud del interesado, cuando esos datos resultan necesarios para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice

[21] Véase el Código Tipo: ACRA.

por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4.1.10. Otros usos que puede darse a la historia social

La historia social, como hemos visto, permite a los trabajadores sociales analizar, sintetizar, describir y cuantificar las situaciones de las personas mayores que se benefician de los servicios sociales. Cualquier otro uso que quiera darse debe ser compatible con los fines es decir cuando se utiliza posteriormente esos datos con fines históricos, estadísticos y científicos y siempre que ese uso posterior se realice de forma disociada. Otros usos tales como de investigación o docencia sólo se podrá realizar siempre que con carácter previo se hayan disociado (art. 5 RLOPD). En todos los demás supuestos, en los que no fuera posible realizar la actividad pretendida con los datos disociados, será obligatorio para la persona que los recabe obtener el consentimiento del titular de los mismos o persona que lo represente legalmente.

4.1.11. La historia social y las cesiones de datos personales

Puede ser posible que los centros y establecimientos asociados, en algún momento, necesiten comunicar los datos de sus residentes a terceros para el cumplimiento de fines directamente relacionados con las funciones legítimas del centro y del tercero. En todos estos casos, conocido también como cesión, la regla general es que siempre se debe contar con el previo consentimiento del interesado titular de los datos. No obstante, dicha norma general no será de aplicación cuando quien permita la cesión de los datos personales se encuentre recogida en una Ley. En este sentido, de acuerdo con lo dispuesto por la Agencia de Protección de Datos de la Comunidad de Madrid y en el Código Tipo ACRA, es posible mencionar algunos supuestos legales existentes[22]:

a) *Cesiones a Órganos Jurisdiccionales o al Ministerio Fiscal:* Con carácter específico, la propia Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, prevé en su artículo 11.2.d) concreta que no será necesario el consentimiento del afectado cuando la comunicación o cesión de datos tenga por destinatario, entre otros, al Ministerio Fiscal o a los Jueces o Tribunales en el ejercicio de las funciones que tiene atribuidas. En estos supuestos es necesario que la petición judicial venga motivada y concrete los documentos de la historia social que sean precisos conocer para su actuación e investigación.
b) *Cesiones a las Fuerzas y Cuerpos de Seguridad:* La LOPD regula este supuesto de forma independiente en el artículo 22.2, y concreta que la recogida y tratamiento de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad para fines policiales se realizará sin consentimiento de las personas afectadas siempre que obedezcan a dos finalidades, como son, la prevención de un peligro real para la seguridad pública o la represión de infracciones penales. Si se trata de datos especialmente protegidos, el propio artículo 22, en su apartado 3, establece que, en estos supuestos, la recogida y tratamiento se podrá realizar exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponda a los órganos jurisdiccionales. El fundamento de este acceso deriva de la actividad de investigación policial reconocida a las Fuerzas y Cuerpos de Seguridad en la Ley Orgánica 2/1986, sobre Fuerzas y Cuerpos de Seguridad del Estado (artículo 11). En cualquier caso,

[22] Son diversos los supuestos en los cuales puede cederse datos, sin embargo, escapa al objeto de este trabajo mencionar todas. Por ello se remite a los distintos supuestos recogidos en las Resoluciones de la Comunidad de Madrid y en el Código Tipo ACRA, entre las que se mencionan la dación de datos a otras residencias o a despachos profesionales o gestorías.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

la actuación policial debe tener un control de legalidad y, consecuentemente, es recomendable que la petición policial venga autorizada y motivada por el órgano judicial correspondiente, con indicación de los documentos de la historia social que sean precisos conocer para la investigación. Sólo cumplidos estos requisitos, el centro puede proceder al envío de una copia de los mismos o facilitar el acceso dentro del propio centro.

c) *Cesiones de datos disociados:* Atendiendo a la regulación prevista en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se define en el artículo 3.f) el término de disociación como todo tratamiento de datos personales, de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. En la medida que los datos personales que obran en la historia social informatizada o no, se comuniquen de forma disociada dejan de tener el carácter de dato personal, y por tanto, de conformidad con lo establecido en el artículo 2.1 LOPD, quedan fuera del ámbito de aplicación de la misma.

d) *Cesiones de datos a otras Administraciones Públicas:* Los datos personales recabados o elaborados en su actividad asistencial por un centro de servicios sociales de titularidad pública no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, si no se dispone del consentimiento previo del interesado. Cuando se trate del ejercicio de la misma competencia o que verse sobre la misma materia, no será necesario el consentimiento del interesado para la cesión de los datos. Tampoco será necesario el consentimiento del interesado para la cesión de los datos a otra Administración Pública cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.

e) *Cesiones de datos a responsables de carácter político:* Los Concejales, en cuanto miembros de las Corporaciones Locales, deben promover la participación de todos los ciudadanos en la vida política, económica y cultural, para lo cual tienen el derecho a obtener del Alcalde, Presidente o Comisión de Gobierno de la Corporación cuanta información precisen para el desarrollo de su actividad. Desde esta perspectiva, podrán acceder a los datos solicitados, sin previo consentimiento de los afectados, siempre que dicho acceso sea necesario para el desarrollo de sus competencias municipales o el ejercicio de sus funciones de control de la Corporación, en los términos previstos en la Ley de Bases de Régimen Local. En estos casos, es imprescindible que la petición de información efectuada por el Concejal, cuando se refiera a datos de carácter personal, se determine de forma clara y precisa la finalidad a la que se van a destinar los datos solicitados y la norma que lo habilita. El acceso a la información por parte de los miembros de la Corporación municipal debe regirse siempre por la obligación de reserva, tal como dispone el artículo 16 del Real Decreto 2568/1986, de 28 de noviembre, de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, que además impone un modo de actuación determinado.

f) *Cesiones de datos a órganos fiscalizadores del gasto público:* En numerosas ocasiones, los responsables de ficheros de la Comunidad de Madrid han planteado a la Agencia de Protección de Datos si es factible ceder datos de carácter personal a la Intervención de la Comunidad de Madrid. En estos casos, la citada Agencia consideró que, de conformidad con lo dispuesto en el artículo 11.2 de la LOPD, la habilitación para ceder datos personales a dicha institución está recogida en el artículo 82 y 83.3.c) de la Ley 9/1990, de 8 de noviembre, de Hacienda de la Comunidad de Madrid. En virtud del primero todos los actos, documentos y expedientes de la Administración de

la Comunidad de los que se deriven derechos y obligaciones de contenido económico serán intervenidos y contabilizados con arreglo a lo dispuesto en dicha Ley y en sus disposiciones complementarias. Por su parte, el artículo 83.3.c) establece como competencia inherente a la función interventora recabar de quien corresponda, cuando la naturaleza del acto, documento o expediente que deban ser intervenidos lo requiera, los asesoramientos jurídicos y los informes técnicos que considere necesarios, así como los antecedentes y documentos para el ejercicio de esta función.

g) *Cesión entre organismos, centros y servicios del Sistema Nacional de Salud*. No es necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

4.1.11. Las medidas de seguridad y el secreto profesional

Todos los ficheros de los que el centro es Responsable deben contar con las medidas de seguridad establecidas por la LOPD y el RLOPD. En este sentido, corresponde a la dirección del centro, como responsable del fichero, designar a la persona responsable de seguridad de los ficheros –sean éstos los expedientes asistenciales o el historial médico- cuya función será la de coordinar y controlar las medidas de seguridad implantadas. Esta designación debería constar en el documento de seguridad y en ningún caso supone una delegación de la responsabilidad dado que ésta siempre corresponde a la dirección del centro como responsable del fichero. Recordemos en este sentido que será al responsable del fichero, y, en su caso, el encargado del tratamiento, el que debe 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.

Igualmente, es preciso indicar que no se podrán registrar datos de carácter personal en ficheros que no reúnan las condiciones que se determinan en el **RLOPD**, con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

En el caso de los historiales médicos y, en su caso, de los expedientes asistenciales, dado que contienen datos de salud del residente y, en algunos caso, también puede contener información relativa a las creencias o a la religión del residente o usuario, como hemos visto, el fichero debe ser calificado como de nivel alto, procurando que los datos reúnan las condiciones necesarias que garanticen su integridad y seguridad, así como respecto de los centros de tratamiento, sistemas, programas, equipos y locales[23].

Esta medida se complementa con la obligación que pesa sobre el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal en tanto que están obligados al secreto profesional respecto de los datos que conozcan en su intervención con el fichero y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. En este sentido, se debe tener en cuenta que para fijar las obligaciones del personal de cada centro, habrá que distinguir entre los profesionales encargados de prestar la asistencia social al usuario del personal de administración y gestión y del personal sanitario que pueda existir en el centro, señalando que con carácter general todos están obligados por

[23] Salvo la excepción contenida en el artículo 79 RDLOPD.

el deber de secreto, deber que con carácter genérico y respecto de los datos de carácter personal viene previsto en el artículo 10 de la LOPD.

4.1.12. Algunos aspectos a tener en cuenta en relación con las medidas de seguridad

La salida de cualquier documento incluido en la historia social fuera de los locales en los que se encuentra la historia, debe ser autorizada con carácter previo por el responsable del fichero. Igualmente, si se tiene previsto trasladar la documentación a otro lugar, corresponde se adopten las medidas de seguridad suficientes para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. En este caso, las medidas que se deban adoptar serán aquellas que el responsable del fichero haya establecido de acuerdo con el RDLOPD.

Igualmente, es preciso señalar, que siempre que se vaya a desechar cualquier documento que contenga datos de carácter personal, es necesario y obligatorio proceder a la destrucción de los mismos mediante la adopción de las medidas dirigidas a evitar el acceso a la información contenida en el documento o la posible recuperación posterior. Se trata de evitar, en el caso de los ficheros no automatizados, el tirar los documentos en los contendores de basura sin que previamente se hayan destruido los mismos.

Asimismo, los armarios, los archivadores u otros elementos en los que se almacenen las historias sociales se deben encontrar en áreas en las que el acceso de las personas esté protegido con puertas dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas también corresponde que permanezcan cerradas cuando no sea preciso el acceso a los documentos incluidos en las historias sociales[24].

4.1.13. Mantenimiento, archivo y cancelación de los historiales sociales de las personas mayores

La dirección del centro, como responsable del fichero de los expedientes asistenciales, es decir de las historias sociales, debe establecer los procedimientos que corresponde adoptar en el archivo de las mismas. Los citados procedimientos deben estar dirigidos a garantizar la correcta conservación de los documentos y su localización así como la consulta de la información en ellos contenida. Igualmente, tienen que posibilitar el ejercicio de los derechos que la LOPD reconoce como son los de acceso, oposición, rectificación y cancelación.

A estos efectos, es preciso diferenciar dos momentos de la historia social.

a) Un primer momento, en el que la historia social está activa por tener utilidad para la debida prestación de asistencia al interesado. En este caso se debe conservar durante el tiempo en que se esté prestando la asistencia y con posterioridad un mínimo de tiempo desde que ésta termine y se considere que puede ser útil para posibles nuevas actuaciones que fuera necesario realizar, y que por equiparación con la historia clínica podría ser de cinco años.
b) El segundo momento sería cuando ha trascurrido el plazo establecido anteriormente y la historia pierde su utilidad desde el punto de vista asistencial, convirtiéndose en pasiva. En este caso, se debe conservar a efectos judiciales de conformidad con la legislación vigente, o cuando existan razones de organización y planificación de los servicios, de investigación o docencia que justifiquen su conservación, en cuyo caso debe enviarse al archivo correspondiente y, en caso contrario, proceder a su destrucción.

[24] Un resumen de las medidas de seguridad consolidadas aplicables a este tipo de ficheros véase en Código tipo ACRA

4.2. La Teleasistencia

La teleasistencia es un servicio básico, en continua evolución que en la actualidad resulta fundamental para procurar a las personas usuarias, generalmente mayores, el desarrollo de su vida en su hogar de manera independiente. Esta finalidad se logra por medio del uso de sistemas basados en TIC, como por ejemplo, el uso de un collarín o pulsera con un emisor que accede telefónicamente a una centralita donde se recibe la llamada de alarma. De esta forma, se buscan soluciones para la vida autónoma de la persona mayor, fomentando los aspectos relacionados con el cuidado y la autonomía personal. Constituye también un elemento que proporciona tranquilidad y seguridad a los familiares de los usuarios de dicho servicio y sobre todo a los mismos usuarios que pasan la mayor parte del tiempo solos o es posible que se encuentren en situaciones habituales de riesgo.

El servicio de teleasistencia se puede definir como *"…un servicio técnico de apoyo e intervención social, enmarcado en el contexto de los servicios sociales de atención primaria, que permite a las personas usuarias, a través de la línea telefónica y con un equipamiento de comunicaciones e informático específico, disponer de un servicio de atención permanente, las 24 horas del día y todos los días del año, atendido por personas específicamente preparadas para dar respuesta adecuada a situaciones de necesidad social o de emergencia"*[25]*.* Dicho servicio puede ser un servicio independiente o complementario al que se reciba de ayuda a domicilio.

La teleasistencia tiene básicamente dos funciones:

a) Proporcionar el auxilio necesario, de forma inmediata, cuando las personas usuarias se encuentran en situación de emergencia y
b) Proporcionar a las personas usuarias tranquilidad y seguridad en el desarrollo de su vida cotidiana, en aquellas otras situaciones que, si bien no constituyen emergencias, necesitan del apoyo de otras personas para su realización.

Para recibir este tipo de prestación, las personas mayores deben facilitar a quien le preste el servicio, unos datos personales a efectos de tramitar su solicitud bien ante la propia administración bien ante las empresas correspondientes. Además, es preciso indicar que durante la prestación del servicio se producirá la grabación de voz del usuario.

Desde el punto de vista de la protección de datos la prestación de este servicio presenta algunos interrogantes, a saber[26]:

Lo primero que se debe afirmar es que la voz de una persona es un dato de carácter personal y, además, si ésta se graba, de acuerdo con la LOPD y normativa de desarrollo, se considera un tratamiento de datos, con lo cual es aplicable todo el régimen de protección de datos y, consecuentemente, es necesario que se inscriba el correspondiente fichero en la Agencia de Protección de Datos correspondiente. El no actuar de esta manera puede suponer, como hemos visto, una infracción leve y, si se recogen sin el consentimiento del titular del dato, grave.

No obstante lo anterior y, dado que el servicio de teleasistencia actúa en muchas ocasiones para solventar una emergencia, resulta en estos casos de aplicación la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en tanto que estamos ante un tipo de comunicación. La citada Ley establece en su Título III, capítulo III el régimen jurídico de la protección de datos personales y de las obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas y concretamente el artículo 38.3 de la misma recoge los derechos que le asisten a los usuarios de los servicios de comunicaciones,

[25] Decreto 144/2011, de 28 de junio, Servicio público de teleasistencia del País Vasco.
[26] Para el desarrollo de este punto se ha tenido en cuenta el Dictamen emitido por la Agencia de Protección de datos del País Vasco, como consecuencia de la consulta planteada por el Departamento de Acción Social de la Diputación de XXXX en relación con el Servicio de Teleasistencia.-CN09-021-.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

dentro de la que se debe destacar la letra d) del citado precepto que dispone *"… sólo se procede al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado".*

El artículo 38.5 de la Ley 32/2003, recoge una excepción, dado que concreta que *"Los usuarios finales no podrán ejercer los derechos reconocidos en los párrafos d) y f) del apartado 3 cuando se trate de llamadas efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen reglamentariamente, en especial a través del número 112"*

Asimismo, la LOPD, como hemos visto, contiene excepciones al consentimiento – art. 6.2- y en el artículo 7.6, relativo a datos especialmente protegidos dispone que "… *podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, 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".*

Con fundamento en los citados artículos, la Agencia de Protección de Datos del País Vasco afirma que *"… tanto el artículo 6.2 con carácter general, como el artículo 7.6, respecto a los datos de salud, permiten una recogida de datos obviando el requisito del consentimiento cuando se trate de proteger un interés legítimo, un interés vital del afectado cuando sea preciso para la prestación de asistencia sanitaria. Es decir, tanto la normativa sectorial en materia de telecomunicaciones, como las normas reguladoras del derecho a la protección de datos de carácter personal permitirían el tratamiento que nos ocupa, sin que fuese preciso una autorización por parte del titular del dato"*

Asimismo, corresponde destacar que las distintas normativas que regulan el servicio de teleasistencia, solicitan de la persona usuaria del servicio distintas autorizaciones, tales como entrada a domicilio, bien sea para su atención, bien para la colocación, mantenimiento o retirada de los equipos. En tales supuestos, cabe señalar, siguiendo el Dictamen mencionado, que las autorizaciones se configuran como obligaciones de los usuarios del servicio lo que determina que la autorización no implica una declaración de voluntad prestada de forma libre. De ahí que se considere que resulta más adecuado, desde el punto de vista de la protección de datos, separar las obligaciones de autorización, de tal modo que la negativa del ciudadano a otorgar las autorizaciones solicitadas no le impida disfrutar del servicio. Se consigue así, una redacción más ajustada al principio de calidad al solicitar de forma obligatoria los datos adecuados, pertinentes y no excesivos. El principio de calidad opera así más que como una limitación del número y tipo de datos que pueden utilizarse, como promotor de un criterio de racionalidad en el manejo de la información.

Finalmente, cuando se contrata el servicio se suele solicitar a los usuarios la autorización para consultar los datos sanitarios y sociales necesarios para la prestación, así como los correspondientes a los datos tributarios, entre otros. En este caso, es preciso señalar que en realidad muchos de los supuestos recogidos como autorizaciones obligatorias no son sino cesiones de datos para las que existe habilitación legal tal como hemos visto en el apartado sobre Cesiones en la historia social al cual remitimos.

4.3. Los datos de la salud de las personas mayores y la historia clínica

4.3.1. El dato de salud y las personas mayores

Como hemos visto, el artículo 7 de la LOPD, recoge un régimen específicamente protector, diseñado por el legislador, para aquellos datos personales que proporcionan una información de las esferas más íntimas del individuo y a los que se califica como "*Datos especialmente protegidos*" –dentro de los cuales se encuentran los datos de carácter personal que revelen ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual- . Se trata de diversas categorías de datos para las que el artículo 7 establece específicas medidas de protección.

Los datos de salud, se encuentran dentro de ésta categoría. El legislador español, de acuerdo con lo dispuesto por el Consejo de Europa (Convenio 108/81, de 28 de enero, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal) y el Derecho Comunitario (Directiva 95/46/CEE, de 24 de octubre relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos), consideró a los datos de salud, como especialmente protegidos y estableció que sólo pueden ser recabados, tratados y cedidos, cuando existan razones de interés general recogidas en una Ley o, el afectado lo consienta expresamente. De esta forma, sólo en los supuestos específicos antes señalados dichos datos podrán ser tratados.

El citado artículo 7.3 de la LOPD concreta la obligación de contar con el consentimiento expreso del afectado, al establecer que:

> "3. Los datos de carácter personal que hagan referencia al origen racial, 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".

Por su parte, el artículo 5.1 g) del Reglamento de desarrollo de la LOPD, define los datos de salud como "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".

En resumen, los datos de salud de las personas mayores son considerados por la LOPD y normas de desarrollo, datos especialmente protegidos (art.7) lo que supone el sometimiento de los mismos a un régimen de especial protección tanto en lo referido a su recogida y tratamiento como en lo que atañe a las medidas que habrán de implantarse sobre los ficheros para garantizar su seguridad y al cumplimiento del deber de secreto que imponen tales normas. De ahí que su difusión y conocimiento por terceros puede afectar a la esfera más íntima de la persona.

4.3.2. Excepción al principio del consentimiento expreso en el caso de los datos de salud.

Como ha quedado expuesto, en el caso concreto de los datos de salud, se requiere para tratar los datos contar con el consentimiento expreso del afectado o de una Ley que así lo disponga por razones de interés general. La LOPD, sin embargo, incorpora en su artículo 7.6 una excepción al principio del consentimiento expreso relativo a datos de salud que acabamos de indicar. El citado precepto dispone que:

> "No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento 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 podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior 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".

El precepto transcrito viene así a posibilitar que los datos relativos a la salud, puedan ser tratados sin las exigencias especiales de protección. Sin embargo, el régimen excepcional contenido en el art. 7.6 antes transcrito, requiere la concurrencia de dos requisitos, a saber:

a) Que el tratamiento de dichos datos "resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios" y que el tratamiento sea "necesario para salvaguardar el interés vital del afectado o de otra persona cuando el afectado esté incapacitado para dar su consentimiento", y
b) Que el tratamiento de datos se realice por un profesional sanitario o por otra persona sujeta a una obligación equivalente de secreto.

4.3.3. La Historia clínica y 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

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 (en adelante, Ley 41/2002, LBrAP), que a su vez, completa las previsiones de la Ley General de Sanidad, define y regula la historia clínica, sin perjuicio, de la normativa que cada Comunidad Autónoma con competencias en materia sanitaria, desarrollen como complemento de dicho texto legal.

La citada Ley 41/2002, LBrAP, en su Capítulo V concreta, en lo que a nosotros interesa, que la historia clínica tiene como fin principal facilitar la asistencia sanitaria. Se trata, indica, de un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente y se compone por un conjunto de documentos relativos a los procesos asistenciales de que sea objeto el citado sujeto. La Historia clínica, para el citado texto legal, también debe incorporar la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.

La Ley 41/2002, LBrAP, refuerza y remarca el reconocimiento del derecho de toda persona a que se respete el carácter confidencial de los datos referentes a su salud, y también a que nadie pueda acceder a ellos sin previa autorización amparada por Ley. Por ello, recoge como principios básicos de la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y documentación clínica, la dignidad de la persona, el respeto a la autonomía de la voluntad y la intimidad.

La historia clínica, también es considerada una fuente de información necesaria para otros muchos fines para los que puede ser útil ajenos al ámbito estrictamente médico. Desde esta perspectiva, la LBrAP, permite que pueda ser utilizada con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, todos ellos considerados fines legítimos y constitutivos de actuaciones fundamentales del Sistema Sanitario, y en función de los cuales la referida Ley también procede a la regulación de su contenido, archivo, tratamiento y uso.

Lógicamente, los datos personales contenidos en todos los documentos e informaciones que forman parte de la historia clínica, sin perjuicio de las previsiones legales propias contenidas en la Ley 41/2002, LBrAP, se encuentran amparados y protegidos por la LOPDC. En efecto, la LOPD, como hemos visto, los define en su artículo 7 como datos especialmente protegidos y recoge un régimen

especialmente riguroso para su obtención, custodia y eventual cesión. Veamos algunos de estos aspectos.

4.3.4. La protección de datos y la historia clínica de las personas mayores

Para la LOPD, un fichero es todo conjunto organizado de datos de carácter personal que permite el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. La historia clínica, desde esta perspectiva, es un fichero que se compone por un conjunto de documentos cualquiera que sea el soporte -papel, audiovisual, informático o de otro tipo- que contiene los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, con identificación de los médicos y demás profesionales sanitarios que han intervenido en él.

Indudablemente, todas las personas mayores cuentan con una Historia clínica, esta puede ser más o menos extensa pero debe contener la narración escrita, de forma clara, precisa, detallada y ordenada de todos los datos antes señalados. Dentro de ella se reflejan los datos personales, como las enfermedades, pasadas o actuales y su estado de salud. En concreto, en la citada historia se deben recoger los datos necesarios sobre la herencia y hábitos de esa persona mayor, su constitución, su fisiología, su psicología, su ambiente y, siempre que sea posible, la etiología y la evolución de la enfermedad. En cualquier caso, cabe señalar que los datos que el personal sanitario recoja en la misma, deben ser siempre adecuados, pertinentes para su finalidad y no excesivos.

Asimismo, es importante destacar que la historia clínica de las personas mayores debe incorporar la información que se considere trascendental para el conocimiento veraz, exacto y actualizado del estado de salud del paciente, a quien a su vez se le reconoce el derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos los procesos asistenciales que sean realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

De acuerdo con la Ley 41/2002, LBrAP, el contenido mínimo de la historia clínica será el siguiente:

a) La documentación relativa a la hoja clínico- estadística
b) La autorización de ingreso.
c) El informe de urgencia.
d) La amnesia y la exploración física.
e) La evolución.
f) Las órdenes médicas.
g) La hoja de interconsulta.
h) Los informes de exploraciones complementarias.
i) El consentimiento informado.
j) El informe de anestesia.
k) El informe de quirófano o de registro del parto.
l) El informe de anatomía patológica.
m) La evolución y planificación de cuidados de enfermería.
n) La aplicación terapéutica de enfermería.
o) El gráfico de constantes.
p) El informe clínico de alta.

Los párrafos b), c), i), j), k), 1), o) y p) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga.

Corresponde a los profesionales sanitarios el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes y a las instituciones asistenciales, llevar la historia con criterios de unidad y de integración, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial.

4.3.5. El responsable del fichero de las historias clínicas

Recordemos que de acuerdo con la LOPD, el responsable del fichero es aquel que decide sobre la finalidad, contenido y uso del tratamiento de los datos. En el caso de las historias clínicas, el responsable será la dirección del centro sanitario, sin perjuicio que, tal como prevé la Ley 41/2002, LBrAP, en aquellos centros con pacientes hospitalizados o que atiendan a un número suficiente de pacientes bajo cualquier modalidad asistencial, la gestión y custodia del fichero se encomiende a una Unidad de Admisión y Documentación Clínica, Unidad que corresponde crear en cada uno de los centros en que exista este tipo de fichero de historias clínicas.

Los criterios básicos de archivo de los citados ficheros de historias clínicas se encuentran contenidos en la citada Ley 41/2002, LBrAP, quien concreta que corresponde a cada centro archivar las historias clínicas de sus pacientes, cualquiera que sea el soporte en el que se encuentre, de manera que quede garantizada su seguridad, su correcta conservación, la recuperación de la información y se posibilite el ejercicio de los derechos que se reconocen al interesado.

4.3.6. La conservación de las historias clínicas de las personas mayores

Todas las historias clínicas, entre las que se encuentran las de las personas mayores, deben ser guardadas por cada institución con criterios de unidad y de integración. De esta manera se facilita el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial. Para logar esta finalidad, es importante que el centro promueva la mayor integración posible de las historias clínicas y, para ello, lo ideal sería que como máximo, en cada centro, exista un único fichero.

Es también importante destacar que corresponde a los centros sanitarios conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad -aunque no necesariamente para ello se deban guardar en el soporte original- para la debida asistencia al paciente durante el tiempo adecuado a cada caso. La LBrAP ha establecido el plazo de cinco años como mínimo para conservar la documentación, plazo que se computa desde la fecha del alta de cada proceso asistencial. Este plazo, no obstante, ha sido modificado por algunas Comunidades Autónomas, como por ejemplo Cataluña y Navarra, que han establecido un periodo mayor, de veinte años. Otras Comunidades Autónomas como Galicia lo han mantenido en cinco, mientras que por ejemplo, Extremadura y Valencia no han establecido un plazo de conservación, con lo cual, corresponde aplicar supletoriamente lo dispuesto por la legislación estatal, es decir, el plazo de cinco años.

En el caso de que los profesionales desarrollen su actividad de manera individual corresponde a éstos la responsabilidad de la conservación, gestión y custodia de la documentación asistencial que generen. En este supuesto, el problema que se puede plantear, es cuando el médico titular de las historias fallece. En este caso, la pregunta que se plantea es ¿a quién corresponde conservarla? La normativa no ha establecido nada al respecto, pero en la práctica, varios Colegios Oficiales de Médicos de España, se han hecho cargo de la custodia de la historia clínica y han facilitado, de esta forma, los accesos a las mismas por los pacientes afectados.

4.3.7. El acceso a las historias clínicas de las personas mayores

Como hemos tenido ocasión de exponer, la historia clínica es un instrumento destinado, fundamentalmente, a garantizar una asistencia adecuada al paciente. Por ello, en primer lugar, los profesionales que asistan a los usuarios se encuentran habilitados por la LBrAP a tener acceso a la citada historia con el fin de poder realizar el diagnóstico o el tratamiento pertinente. De ahí que es importante que cada centro establezca los métodos que posibiliten, en todo momento, el acceso a la historia clínica por parte de los profesionales que le asisten.

Igualmente, existe determinado personal que trabaja en el Centro que también tiene, en determinados momentos, que acceder a la historia clínica. Se trata del personal de administración y gestión de los centros sanitarios pero el acceso a la misma sólo puede autorizarse para acceder a los datos recogidos en la historia clínica necesarios para el desarrollo de sus propias funciones. Corresponde en este caso, al responsable del fichero establecer las características de dicho acceso que, en todo caso, deben respetar, además de las limitaciones impuestas por la LBrAP, lo establecido por la normativa autonómica correspondiente.

Por otra parte, el personal sanitario que se encuentre debidamente acreditado y que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene también reconocido por la LBrAP el acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia.

En todos los casos, el acceso a los datos se debe realizar con pleno respeto de los derechos del paciente o de cualquier otra obligación impuesta por el centro en relación con los pacientes y usuarios o de la propia Administración sanitaria. Igualmente, es preciso señalar, que tanto los profesionales como cualquier otro personal que acceda a los datos recogidos en la historia clínica queda sujeto al deber de secreto. Dicho deber, recogido en el artículo 10 de la LOPDC, supone, de acuerdo con el citado precepto que:

> "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

Finalmente, también la LBrAP permite que otros sujetos, distintos a los señalados con anterioridad, tengan acceso a la historia clínica cuando deban cumplir determinadas funciones. En este sentido, permite que accedan a la historia clínica cuando se persigan fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia. En todos estos casos, el régimen aplicable de acceso será el contenido en la LOPDC, la Ley General de Sanidad, y demás normas de aplicación en cada caso. De acuerdo con dicha normativa, el acceso a la historia clínica con los citados fines obliga, en todo caso, 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. Quedan exceptuados de la citada regla los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en cuyo caso se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. En cualquier caso, es preciso indicar que el acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

4.3.8. El caso especial de acceso a la Historia clínica de una persona mayor fallecida

En muchas ocasiones, se puede plantear la necesidad de acceder a los datos de una persona anciana fallecida. Este acceso puede ser solicitado bien por el cónyuge bien por cualquier otro familiar. Dado que los datos contenidos en dicha historia ya no

corresponden a una persona física –ámbito de aplicación de la LOPD– la pregunta que surge es la siguiente: ¿Es aplicable la legislación de protección de datos a una persona fallecida?

Lo primero a destacar es el ámbito de aplicación de la LOPD. Recordemos que de conformidad con la citada normativa de protección de datos, su ámbito de aplicación se circunscribe a los datos de las personas físicas y, consecuentemente, una persona fallecida, ha dejado de serlo. Por otra parte, los derechos de acceso, rectificación y cancelación de los datos personales se configuran por la LOPD como derechos personalísimos y, consecuentemente, únicamente pueden ser ejercitados directamente por el propio afectado –salvo los supuestos permitidos de representación-. La LOPD no expresa nada respecto del acceso a dicho datos, pero el artículo 2.4 del RLOPD, vino a disipar esta laguna y dispone que

> "este Reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".

En consecuencia, con carácter general, no será aplicable al tratamiento de los datos personales del fallecido las normas de la LOPD. No obstante, la afirmación debe ser matizada, dado que dependiendo del tipo de datos que se quiera acceder, puede existir una legislación especial aplicable al caso que deba ser tenida en cuenta. En efecto, si se trata de acceder al historial clínico, es preciso valorar lo establecido en el artículo 18.4 de la Ley 41/2002, LBrAP que dispone:

> "Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros."

En este caso, se debe por tanto analizar la referencia efectuada por el citado precepto a las personas vinculadas a los fallecidos "por razones familiares o de hecho". A tal efecto, es preciso tener en cuenta lo dispuesto en el artículo 4 de la Ley Orgánica 1/1982, de 5 de mayo, reguladora de la protección civil de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen, que establece lo siguiente:

> "1. El ejercicio de las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida corresponde a quien ésta haya designado a tal efecto en su testamento. La designación puede recaer en una persona jurídica.
>
> 2. No existiendo designación o habiendo fallecido la persona designada, estarán legitimados para recabar la protección el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento.
>
> 3. A falta de todos ellos, el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal, que podrá actuar de oficio o a instancia de persona interesada, siempre que no hubieren transcurrido más de ochenta años desde el fallecimiento del afectado. El mismo plazo se observará cuando el ejercicio de las acciones mencionadas corresponda a una persona jurídica designada en testamento."

La interpretación más extensiva de dicho precepto permite, a lo sumo, entender ampliado el ámbito previsto en sus apartados 1 y 2 a las personas que mantuvieran con el fallecido una relación de hecho similar a la derivada del matrimonio así como a los herederos del fallecido que aún no siendo designados expresamente por aquél en su testamento, pretendiesen el ejercicio de las acciones a las que se refiere la mencionada Ley.

De este modo, una interpretación del artículo 18.4 de la Ley Orgánica 41/2002 antes transcrito coherente con el contexto normativo en el que la misma fue aprobada permitiría el ejercicio del derecho de acceso a la historia clínica del fallecido por parte de su cónyuge o persona vinculada con aquél por una relación de hecho similar, ascendientes y descendientes, así como las personas que hubieran sido designadas por el fallecido para ejercer las acciones a las que se refiere la Ley Orgánica 1/1982 y, en última instancia, sus herederos que además se encontrasen vinculados a aquél por relaciones familiares o de hecho análogas a la familiar.

Por tanto, el acceso a los datos de una persona fallecida sólo podrá ser posible cuando quien lo solicite hubiera sido designado por la misma para el ejercicio de las acciones previstas en la Ley Orgánica 1/1982 o tuviera la condición de heredero de la persona fallecida.

También será posible el acceso a los datos, si el solicitante actúa en nombre y representación de la persona fallecida, en cuyo caso, será preciso que la persona acredite el apoderamiento o la condición de heredero a las que se ha hecho referencia.

4.3.9. Las medidas de seguridad que deben tener las historias clínicas

La LOPD impone al responsable del fichero la adopción de medidas de seguridad cuyo detalle se contiene en las normas reglamentarias que la desarrollan. En efecto, el artículo 9 de la LOPD señala:

> "1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garantice 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.
>
> 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
>
> 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El RLOPD ha sido la norma que vino a concretar la determinación del nivel de seguridad aplicable a los ficheros. El Título VIII del citado reglamento lleva por rúbrica *"De las medidas de seguridad en el tratamiento de datos de carácter personal"* y el Capítulo I del mismo, regulador de las Disposiciones generales, concreta el alcance, los niveles de seguridad y la aplicación de las medidas a los ficheros. En efecto, el artículo 79 del RLOPD establece que:

> "Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento."

Por su parte, el artículo 80 determina que:

> "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto."

Por último, el artículo 81 regula la aplicación de los niveles de seguridad. En lo que a este trabajo interesa, el artículo 81.3 del RLOPD, prevé que los ficheros que contengan datos de salud, deberán reunir, además de las medidas de nivel básico y medio, las medidas calificadas como de nivel alto, concretadas por el citado reglamento en los artículos 101 y ss. Sin entrar en un estudio exhaustivo sobre el tema baste señalar que, entre las medidas de seguridad que corresponde implantar por parte de los distintos centros asistenciales en relación con la custodia y el acceso a los ficheros de las historias clínicas, es la de garantizar la confidencialidad

de los datos contenidos en ella y la de evitar los accesos no autorizados. Para ello, es preciso controlar quién está utilizando la historia desde la salida del fichero hasta la devolución de la misma. Las citadas medidas se deben documentar necesariamente por escrito y será responsabilidad de cada centro la elaboración del documento de seguridad, su difusión y su conocimiento por todo el personal que pueda o vaya a tener participación en la gestión, manejo o utilización de las historias clínicas.

Igualmente, es importante destacar que todo el personal que acceda a los ficheros de las historias clínicas no tienen las mismas obligaciones salvo, la de carácter general, relativa al deber de secreto, deber que con carácter genérico y respecto de los datos de carácter personal viene previsto, como ya hemos visto, en el artículo 10 de la LOPD.

En todo caso, es preciso que cada centro proceda a distinguir entre los distintos profesionales de la sanidad que asisten al paciente de aquel que acceda como personal de administración y de gestión del centro. De esta forma, los profesionales asistenciales que realicen el diagnóstico o el tratamiento de la persona mayor, tendrá acceso a la historia clínica completa como instrumento fundamental para su adecuada asistencia. Por su parte, el personal de administración y gestión de los centros e instituciones sanitarias sólo podrán acceder a los datos de la historia clínica relacionados con sus propias funciones que pueden estar relacionadas, por ejemplo, con la admisión del paciente, cita previa, funciones contables, presupuestarias, etc..

4.4. La videovigilancia y los datos captados de las personas mayores

4.4.1. Objetivos que se pretenden conseguir

Suele ser usual que en las residencias de las personas de la tercera edad o en los centros asistenciales, cuenten con sistemas de videovigilancia. Normalmente, los motivos que se suelen esgrimir por parte de los responsables de las citadas instituciones para la instalación de los sistemas de video-vigilancia suelen estar ligados a la necesidad de controlar las incidencias de seguridad que puedan ocurrir durante veinticuatro horas con los residentes del centro. Fundamentalmente, los responsables de los centros justifican el uso de estos sistemas en la necesidad de velar por la integridad física y seguridad de los usuarios del centro dado que se trabaja con personas de edad avanzada, que requieren una atención especializada ya que, en algunos casos, padecen enfermedades con trastornos mentales (como puede ser el Alzheimer) o discapacidades importantes lo que puede suponer actuaciones imprevisibles en sus formas de actuar, como por ejemplo abandonar el centro. En consecuencia con este tipo de instalación se consigue el bienestar y, sobre todo, la seguridad de sus residentes.

Ahora bien, la instalación y uso de cámaras o videocámaras no es admisible en todos los casos sino sólo cuando no exista un medio menos invasivo a la intimidad de las personas y de acuerdo con el principio de proporcionalidad.

4.4.2. Algunos aspectos a considerar en relación con la videovigilancia y las personas mayores

De acuerdo con la LOPD, la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y la Guía de videovigilancia aprobada por la AEPD, dentro del concepto de dato personal, se debe considerar incluido las imágenes cuando se refieran a personas identificadas o identificables. A partir de dicha consideración, los principios vigentes en materia de protección de datos personales se deben aplicar al uso de cámaras, videocámaras y a cualquier medio técnico análogo, que capte y/o registre imágenes, ya sea con fines de vigilancia u otros, en los supuestos en que:

a) Exista grabación, captación, transmisión, conservación, o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquéllas.
b) Tales actividades se refieran a datos de personas identificadas o identificables.

En este sentido, la Guía de Videovigilancia concreta que la utilización de la videovigilancia para captar, grabar o reproducir imágenes relativas a personas identificadas o identificables constituye una práctica que puede afectar a los derechos fundamentales y en particular al derecho fundamental a la protección de datos. Por ello, considera que se debe tener en cuenta algunas consideraciones:

a) La elección de este tipo de medios debe responder siempre al principio de proporcionalidad descartándose la videovigilancia cuando existan medidas menos lesivas para los derechos fundamentales.
b) El análisis de la proporcionalidad de la medida será especialmente riguroso en entornos sensibles ya sea por la naturaleza de los sujetos objeto de la vigilancia, como es el caso de los mayores de edad, en tanto que en ellos se pueden dar manifestaciones de vida privada.
c) En caso de utilizar la videovigilancia con fines de seguridad privada deberá recurrirse siempre a empresas de seguridad que debe reunir todos los requisitos legales para ello.
d) Por su parte, la empresa de seguridad debe asesorar diligente y lealmente a quien requiera sus servicios incluyendo dicho asesoramiento en las cuestiones relativas a la normativa de protección de datos y será responsable y encargada de velar por el cumplimiento de la normativa de protección de datos personales y cualquier otra norma aplicable.

4.4.3. Información que debe proporcionar el centro que tenga instalado un sistema de videovigilancia

Todos los centros que tengan instalado un sistema de videovigilancia están obligados, de acuerdo con la LOPD, a informar a todas las personas, residentes o no, de la existencia del sistema a través de un cartel claramente visible. Dicho cartel no puede ser cualquiera, sino únicamente aquel que se encuentra recogido en el anexo de la Instrucción 1/2006 en el que figura, como vemos una cámara acompañada de la leyenda "ZONA VIDEOVIGILADA". El cartel tiene como finalidad principal servir para que todas las personas que transiten por los lugares vigilados se encuentren informadas de que están siendo vigiladas.

A quien corresponde instalar el cartel y cumplir con el deber de información establecido en el artículo 5 de la LOPD es al responsable y para logar el cumplimiento de este deber, los responsables deben:

a) Colocar, en las zonas videovigiladas al menos un distintivo informativo ubicado en lugar suficientemente visibles, tanto es espacios abiertos como cerrados y
b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la LOPD.

En cuanto al contenido y diseño del distintivo informativo, como se puede observar es preciso destacar:

a) El distintivo informativo a que se refiere el artículo 3.a) de la Instrucción debe de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS»

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

b) También deberá contener una mención a la finalidad para la que se tratan los datos
c) Debe contener una indicación que indique «ZONA VIDEOVIGILADA»
d) Igualmente debe hacer mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la LOPD[27].

El no contar con el distintivo puede dar lugar a la imposición de una sanción de carácter grave o, si se trata de la primera vez, a un apercibimiento. El artículo 44.3.c) de la LOPD, considera infracción grave "*Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave*, infracción sancionada con multa de 40.001 a 300.000 euros (45.2 LOPD).

4.4.4. El acceso a la información del usuario, conservación de los datos y cámaras falsas

La LOPD, reconoce a todas las personas mayores que se encuentren en el centro, así como aquellas que las acompañan, el derecho a solicitar al centro que tenga instalado un sistema de videovigilancia, información sobre la captación de su imagen y la finalidad que motiva la misma. La Instrucción 1/2006 citada, establece que el cartel informativo -descrito anteriormente- es el que cumple con aquel derecho de información y se debe ubicar como mínimo en los accesos a las zonas vigiladas, sean estos exteriores o interiores y si el lugar dispone de varios accesos se debe colocar en todos ellos con el objeto de que la información que se proporciona sea visible con independencia de por donde se acceda.

Las imágenes captadas por los sistemas de videovigilancia se deben conservar sólo por el tiempo imprescindible para la satisfacción de la finalidad para la que se recabaron, tiempo que nunca puede superar el plazo de un mes. Durante ese plazo de tiempo, la imagen debe estar protegida a través de las correspondientes medidas de seguridad, con el fin de permitir el acceso sólo a las personas autorizadas y, a su vez, evitar que personas ajenas al centro residencial tengan acceso[28].

En relación con las cámaras instaladas que no funcionan la AEPD concretó que no es posible acreditar que dichas cámaras graben, por ello, como no se puede probar la captación y grabación de imágenes y teniendo en cuenta el principio de presunción de inocencia, declara en la mayoría de las actuaciones, el archivo de las mismas[29].

4.4.5. Principios de calidad, proporcionalidad y finalidad del tratamiento

El artículo 4 de la citada Instrucción 1/2006, titulado "Principios de calidad, proporcionalidad y finalidad del tratamiento", dispone que:

a) Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.
b) Sólo se considera admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para

[27] Artículo 3 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
[28] Informe 0472/2009.
[29] Expediente Nº: E/00888/2007; Procedimiento Nº PS/00287/2008.

la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

c) Las cámaras y videocámaras 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 todo caso se debe evitar cualquier tratamiento de datos innecesario para la finalidad perseguida.

Para el efectivo cumplimiento de los principios indicados, en especial los relativos a la proporcionalidad y finalidad de los medios utilizados para el servicio de video-vigilancia, se debe señalar que, no es recomendable que los dispositivos instalados tengan la capacidad de captar o registrar tanto imágenes como sonidos mediante técnicas desproporcionadas para la finalidad del tratamiento, como pueden ser dispositivos móviles, direccionables, de ampliación de imágenes o posibilidad de enfoque de imágenes ajenas a la finalidad concreta y específica de video-vigilancia.

4.4.6. El lugar donde pueden y deben ubicarse las cámaras de videovigilancia

Las cámaras y videocámaras sólo pueden ser instaladas en espacios privados y no pueden obtener imágenes de espacios públicos, dado que en este caso la competencia es exclusiva de los Cuerpos y Fuerzas de Seguridad del Estado de conformidad con lo dispuesto en la Ley Orgánica 4/1997, de 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado[30]. Excepcionalmente, puede grabar imágenes en espacios públicos cuando resulte imprescindible para la finalidad de vigilancia que se pretende o resulte imposible evitarlo por razón de la ubicación de aquéllas. Siempre se debe evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

La instalación de las videocámaras tampoco se podrá realizar en lugares que puedan ser lesivos para la dignidad personal, tales como el interior de las habitaciones.

El artículo 44.2.c) de la Ley Orgánica 15/1999 considera infracción leve: *"El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesad",* sancionable con multa de 900 a 40.000 euros.

4.4.7. Sistemas de grabación de imágenes a través de los videoporteros

Cuando la imagen de una persona se realiza a través de un videoportero se encuentra excluida del ámbito de aplicación de la LOPD e Instrucción 1/2006, de 8 de noviembre, dado que nos encontramos ante imágenes captadas en un ámbito personal y doméstico, entendiéndose por tal, el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar. En efecto, en estos casos la finalidad no es de vigilancia sino de identificación de la persona. Por ello, en virtud del artículo 2 de la LOPD, se encuentra excluida del ámbito de aplicación de la LOPD.

No obstante lo anterior, la AEPD diferenció dos supuestos:

a) Aquellos casos en los que la utilización de videoporteros se limita a verificar la identidad de la persona que llamó al timbre y, en su caso, a facilitar el acceso a la vivienda., en cuyo caso, lo consideró una actividad domestica y por tanto no será de aplicación la normativa sobre protección de datos.

b) Aquellos en los que el servicio de videoporteros se articula mediante procedimientos que reproducen y/o graban imágenes de modo constante, y resultan accesibles -ya sea a través de Internet o mediante emisiones por la televisión de los vecinos-, y en particular cuando el objeto de las mismas

[30] Procedimiento Nº PS/00208/2007.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

alcance al conjunto del patio y/o a la vía pública colindante. En este supuesto se considera de plena aplicación la LOPD y la Instrucción 1/2006[31].

4.5. Fuentes accesibles al público

4.5.1. Planteamiento de la cuestión

Es normal, que una persona de la Tercera Edad que vive en su domicilio cuente con un teléfono y aparezca en la guía telefónica, es decir, que figure en una de las denominadas fuentes accesibles al público. El uso que de éstos puedan hacerse, los derechos que la LOPD les reconoce y la regulación que le es aplicable será el objeto de este apartado.

Como hemos visto, la regla general que rige para cualquier tratamiento o cesión de datos conforme la LOPD y sus normas de desarrollo, es que todo tratamiento de datos personales precisa del *"consentimiento"* del afectado, salvo que la LOPD disponga lo contrario. El propio artículo 6, apartado 2 de la LOPD señala aquellas excepciones. En lo que aquí interesa dispone:

> "No será preciso el consentimiento……. cuando los datos figuren en *fuentes accesibles al público* y su tratamiento sea 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". De acuerdo con el artículo 3 j) de la LOPD son 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 consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y 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. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación".

De la definición trascrita es posible verificar que aparentemente existe una contradicción en el precepto dado que el primer inciso tiene carácter genérico y no limitativo al concretar que son fuentes accesibles al público las que pueden ser consultadas por cualquier persona, previo pago, en su caso, de una contraprestación y, siempre que la accesibilidad no esté impedida o limitada por ninguna norma jurídica. No obstante, inmediatamente la norma establece el criterio de lista cerrada, dado que considera que tienen, "exclusivamente", la característica de fuentes accesibles al público, en nuestro caso, los repertorios telefónicos en los términos previsto en su normativa específica, entre otros.

Numerosas resoluciones de la Agencia Española de Protección de Datos se han encargado de aclarar esta aparente contradicción[32] que finalmente ha sido resuelta por el artículo 7 del RDLOPD al mejorar la redacción. El citado precepto señala que *"sólo tendrán el carácter de fuentes accesibles al público:….b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica……* Y punto y aparte, indica que *"En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación".*

[31] Véase el Informe 0294/2009, donde destaca la AEPD que cuando una cámara permite reproducir en tiempo real las imágenes que concurren en la portería de un edificio, su actuación excede con mucho del ámbito personal y doméstico, por lo que implica un tratamiento de datos de carácter personal, que conlleva la necesidad de legitimar dicho tratamiento en los términos del artículo 2 de la Instrucción.

[32] Muchas son las resoluciones que han aclarado este precepto, entre las que cabe destacar la Resolución R/00133/2005, recaído en el procedimiento sancionador PS/00170/2004.

Centrándonos en el tema de los repertorios telefónicos, es preciso indicar que la regulación de la LOPD se debe completar con la normativa específica que regula este tipo de guías, en nuestro caso, por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y en el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, que complementó la transposición a nuestro ordenamiento jurídico de la Directiva de servicio universal.

4.5.2. Las guías o repertorios telefónicos

La regulación de las guías telefónicas como los servicios disponibles al público se contiene, como hemos visto, en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones –en adelante LGT- y en el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. Aquella normativa, establece que tanto en la guía telefónica como en los servicios de información telefónica, todos los abonados al servicio disponible al público, entre los cuales se encuentran las personas mayores, tienen derecho a "ser" o "no ser" incluidos en ella y a que se les entregue una guía general –impresa o electrónica- donde se ofrezca información sobre todos los números de abonados. En igual sentido, se concreta la obligación de prestar un servicio de información general de números de abonados a todas las personas por medio de la cual se facilite el número telefónico de un abonado.

En todos estos supuestos, los operadores habilitados para tratar los datos de carácter personal deben cumplir la normativa que desarrolla el Derecho Fundamental a la Protección de Datos, regulado por la LOPD y por su norma de desarrollo, el RDLOPD.

Recordemos en este sentido que de acuerdo con el art. 3, a) de la LOPD, los datos personales son definidos como "*cualquier información concerniente a **personas físicas** identificadas o identificables*" (destacado nuestro). Estos datos, para ser tratados, deben ser incluidos en un fichero, considerado por la propia norma (artículo 3.b).), como "*conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*". El fichero que así se vaya a constituir, se encuentra sometido a la LOPD y, consecuentemente, es obligatoria su inscripción en el Registro General de Protección de Datos[33]. De ahí que los ficheros que se elaboren para la confección de las guías telefónicas o para la prestación de los servicios de información, se encuentren sujetos a esta normativa.

El fichero con los datos, debe cumplir con los principios de protección de datos recogidos en la LOPD, es decir, con la calidad de los datos, el derecho de información en la recogida de los mismos, el principio de datos especialmente

[33] El artículo 26 de la LOPD, titulado Notificación e inscripción registral que: *"Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, 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. Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá 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 Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos."*
En consecuencia, la notificación de los ficheros siempre debe ser previa a la creación de los mismos, por lo que la ausencia de dicha notificación sería una conducta constitutiva de infracción leve, con arreglo a lo dispuesto en el artículo 44.2.c) de la propia Ley.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

protegidos, la seguridad de los datos, el deber de secreto, la comunicación de los datos y el acceso a los mismos por cuenta de terceros.

4.5.3. La confección de las guías telefónicas y de servicios de comunicaciones electrónicas y la protección de datos. Requisitos que se deben tener en cuenta

En los procedimientos de confección de las guías telefónicas y las guías de servicios de comunicaciones electrónicas disponibles al público, las empresas habilitadas para ello, como responsables del tratamiento, deben cumplir con varias exigencias. En cualquier caso, es preciso indicar, que la existencia de una entidad intermediaria, que elabore la guía por encargo del operador habilitado, es decir, los denominados encargados del tratamiento – ex artículo 12 LOPD-, no excluye, bajo ningún concepto, la responsabilidad del operador habilitado.

Cuando los datos de los abonados son usados en la confección de las guías, bien por los operadores bien por los intermediarios, es preciso tener en cuenta las siguientes cuestiones:

1. La primera inclusión de datos de abonados en cualquier tipo de guía de abonados, incluida la de servicio universal, sea esta electrónica o impresa, que se encuentre disponible al público o accesible a través de servicios de información o de consulta sobre ella, se debe realizar siempre con el consentimiento expreso del abonado.
2. Sólo se considera que existe consentimiento expreso del abonado cuando éste haya respondido dando su aceptación o el propio abonado haya solicitado su inclusión.
3. Una vez que el abonado ha otorgado el consentimiento, las sucesivas inclusiones de los datos del abonado o, en su caso, la cesión de los mismos a otra entidad para incluirlo en un Directorio o para la prestación de servicios de información o de consulta sobre la guía, no precisa de consentimiento expreso, siempre que la cesión cumpla los requisitos de la LOPD. En este caso, en principio tan sólo es necesario que, en el plazo de un mes contado desde la comunicación en la que se le solicita el consentimiento, el abonado no se oponga expresamente
4. En todo caso, es preciso informar, con carácter previo al abonado, sobre los datos que se prevén incluir, la finalidad de la guía o Directorio y el modo en el que serán incluidos en las mismas.
5. Los datos que, como mínimo, deben figuran en las guías, son los relativos a nombre y apellidos o razón social, número o números de abonado, dirección postal del domicilio, excepto piso, letra y escalera, identificador del tipo de terminal específico (en su caso, tal como teléfono normal, fax, RDSI, etc.) y nombre del operador que facilite el acceso a la red.
6. Se reconoce también el derecho de los abonados a exigir a los operadores y proveedores a no figurar en las guías telefónicas. En este caso, los citados datos sólo serán proporcionados a las entidades titulares de servicios de atención de llamadas de emergencia.
7. Igualmente, tienen derecho a que alguno de los datos antes mencionados se puedan omitir parcialmente en los términos estipulados por su proveedor, tales como su dirección u otros datos personales
8. Si el abonado es una persona física se permite que, asociado a un mismo número, figure el nombre de otra persona mayor de edad con la que conviva. En este caso, es preciso que la persona que vaya a figurar otorgue su consentimiento, en los términos antes expuestos.
9. Es posible la inclusión en las guías, tanto impresa como electrónica, de cualquier otro dato distinto a los mencionados en el apartado a), siempre que se cuente con el consentimiento expreso del abonado, pero en este

caso, dicho consentimiento es preciso tanto en la primera inclusión como en las sucesivas.

10. Se reconoce el derecho a los abonados para que los datos que aparecen en la guía no sean utilizados con fines de publicidad o prospección comercial. A tal efecto se obliga a que en la guía conste esta circunstancia de forma clara. Cualquier utilización que se realice con esta finalidad constando la oposición expresa en la guía supone la vulneración de lo establecido en la LOPD
11. Se reconoce a los abonados el ejercicio de los derechos de acceso, rectificación, oposición y cancelación de los datos en los términos previstos en la LOPD sin que, en ningún caso, el ejercicio de los mismos pueda suponer ingreso alguno para el sujeto obligado.
12. Cuando se ejercite los derechos antes señalados por los abonados en relación con las guías telefónicas, las rectificaciones, cancelaciones, oposiciones, aceptadas se deben hacer extensibles a los servicios de consulta sobre números de abonado, salvo manifestación en contra del propio abonado.
13. Si se trata de guías telefónicas en formato electrónico, éstas nunca pueden permitir obtener la identidad o el domicilio de un abonado a partir de su número de teléfono u otro recurso identificativo de abonados, es decir, la identificación inversa.

4.5.4. Las guías telefónicas como fuentes accesibles al público

Como hemos visto, la regla general que rige para cualquier tratamiento o cesión de datos conforme la LOPD y sus normas de desarrollo, es que todo tratamiento de datos personales precisa del *"consentimiento"* del afectado, salvo que la LOPD disponga lo contrario. El propio artículo 6, apartado 2 de la LOPD señala aquellas excepciones y expresa que "*No será preciso el consentimiento… cuando los datos figuren en* ***fuentes accesibles al público*** *y su tratamiento sea 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*".

Recordemos también que toda cesión o comunicación de datos a terceros sólo se podrá realizar para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. El artículo 11.2 de la LOPD, también indica, en relación con la cesión de datos que *"El consentimiento exigido… no será preciso… b) Cuando se trate de datos recogidos de fuentes accesibles al público".* Las citadas excepciones son también recogidas en el artículo 10.2.b) del Reglamento cuando establece que *"….será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando……a) Lo autorice una norma con rango de ley o una norma de derecho comunitario…….b) Los datos objeto de tratamiento o de cesión figuran 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 tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*

En consecuencia, de los preceptos transcritos, parece claro que todo tratamiento o cesión de datos por parte de un tercero que se encuentren recogidos en una fuente accesible al público, en nuestro caso, una guía telefónica o una guía de servicios, no precisan para acceder y registrar los datos en un fichero por parte de un tercero del consentimiento del interesado. Se trata de un límite al ejercicio del Derecho Fundamental reconocido por el artículo 18.4 de la CE y, como toda limitación, cualquier interpretación de la norma limitadora ha de efectuarse en forma restrictiva, sin exceder de aquello específicamente previsto en la misma.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

4.5.5. Un proceso importante; la incorporación de los datos obtenidos de las guías de comunicaciones electrónicas a un fichero

Como ha quedado expuesto, el dato que se obtiene de una fuente accesible al público y, consecuentemente de una guía telefónica, no requiere para su tratamiento del consentimiento del titular del dato. No obstante, es preciso indicar que el dato así obtenido sólo puede ser tratado, cuando sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero al que se incorpora o por el tercero a quien se comuniquen dichos datos. Esta afirmación supone que cualquier persona no se puede apropiar de los datos que figuran en dichas fuentes y registrarlo en un fichero sin más justificación, es decir, por el sólo hecho de que aparezcan en las mismas. La propia LOPD se encarga de poner un límite a dicho acceso y obliga, tanto al responsable del fichero que se apropia del dato, como al tercero a quien se le comunican, a obtener los datos de las citadas fuentes exclusivamente para la satisfacción, como ya hemos dicho, del interés legítimo que éstos persigan. Corresponde entonces preguntarse ¿cómo se puede comprobar la consecución de aquel interés legítimo?

La comprobación de que concurre aquella circunstancia se debe realizar teniendo en cuenta las finalidades reconocidas al fichero donde se registran los datos obtenidos de la fuente de acceso público, de tal forma que sólo pueden ser recogidos para cumplir las finalidades determinadas, explícitas y legítimas del responsable del tratamiento sin que se pueda utilizar los datos para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Por tanto, los datos que se encuentran en una fuente accesible al público no son datos de libre acceso.

Pero, además de que el responsable del fichero acredite un interés legítimo, es preciso, tal como lo exige la regulación de protección de datos, que aquél compruebe la calidad de los datos obtenidos de la fuente accesible al público que vaya a incorporar a su fichero (art. 4 LOPD y 8 RLOPD). En este sentido, corresponde al responsable verificar que los datos obtenidos son exactos y están puestos al día, de forma tal que respondan con veracidad a la situación actual del afectado. Esta obligación pesa sobre el responsable del fichero que va a incorporar el dato obtenido de la fuente accesible, quien de oficio debe verificar, en todo momento, que el dato obtenido e incorporado al fichero y sometido a tratamiento no es inexacto, en todo o en parte, o incompleto. Si detectara alguna de estas irregularidades le corresponde sustituirlo por los correspondientes datos rectificados o completados o, en su caso, cancelarlo en un plazo de diez días contados desde la fecha en que tenga conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello. Por ello, si el dato obtenido cambia en algún momento su naturaleza, es decir, que deja de ser un dato incluido en una fuente accesible al público (caso, por ejemplo, de publicarse unas nuevas guías telefónicas) corresponde al responsable proceder a la cancelación del mismo de oficio (art. 4 LOPD).

Igualmente, se debe señalar, que el responsable del fichero debe verificar, en todo momento, que los datos obtenidos de las fuentes accesibles al público e incorporados a su fichero no hayan dejado de ser necesarios o pertinentes para la finalidad para la cual han sido recabados o registrados. Si comprueba tal circunstancia, debe proceder a cancelarlos[34].

En todo caso, debe quedar claro que los datos obtenidos de una fuente accesible al público se incorporan a un fichero y el producto resultante, es decir, el fichero donde se introducen los datos, es otro fichero que no tiene, bajo ningún concepto, el carácter de fuente accesible al público. Esto supone que el fichero resultante

[34] Sin embargo, debe conservarlos 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.

debe, en todo caso, adecuar su tratamiento a las disposiciones de la LOPD y a sus normas de desarrollo[35].

El artículo 6.2 de la LOPD, cierra su redacción exigiendo que toda recopilación o transmisión de los datos obtenidos de fuentes accesibles al público y la posterior introducción del dato en un fichero, no vulnere los derechos y las libertades públicas, previsión que también es reiterada por el artículo 10.2.b) del Reglamento y que se debe entender en el sentido establecido por la Sentencia del Tribunal Constitucional nº 292/2000, de 30 de noviembre, en tanto que reconoce que "… *El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.".* De ahí que la protección no se ciña tan sólo a los derechos fundamentales en sentido estricto, sino que va más allí, protegiendo también "*cualquier otro bien constitucionalmente amparado".*

Igualmente, es preciso indicar que como hemos visto, de acuerdo con el artículo 6 LOPD y 12 del RLOPD, corresponde al responsable del fichero acreditar, en todo momento, que el dato se ha obtenido de una fuente accesible. Esta prueba es esencial, dado que se trata de un supuesto excepcional de exigencia del consentimiento del interesado contemplado por la LOPD que como hemos visto, configura el principio del consentimiento como principio básico en materia de protección de datos reiterado en la Sentencia 292/2000, de 30 de noviembre, del TC. Si el responsable no puede demostrar aquellas circunstancias, se entiende vulnerado el principio de consentimiento que la ley consagra y, por tanto, incurre en infracción grave tipificada en el artículo 44.3.c) de la LOPD al "*Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave*" infracción sancionada con multa de de 40.001 a 300.000 euros[36].

La AEPD así lo ha entendido en varias ocasiones al considerar que la empresa "*… no ha justificado la procedencia de los datos del denunciante de la "guía telefónica", máxime, cuando, la estructura de la copia facilitada tampoco coincide con el formato de dichos repertorios de abonados, lo que le lleva a concluir en todos los caso que los datos no proceden de una fuente accesible al público, en los términos previstos en el artículo 3.j de la LOPD"*[37]. En parecidos términos, otra resolución de la misma entidad considera que "*…no ha acreditado que contara con el consentimiento de los afectados para tratar sus datos. No ha acreditado de dónde ha obtenido los datos personales de los colegiados que obran en su archivo… No ha especificado de qué repertorios telefónicos ni de qué anuarios de colegiados los*

[35] Ejemplo de ello, lo constituye la Resolución: R/00862/2008, recaída en el procedimiento sancionador PS/00002/2008, instruido por AEPD.

[36] La Audiencia Nacional ha manifestado en su Sentencia de 22 de octubre de 2003 que "*la descripción de conductas que establece el artículo 44.3d) de la Ley Orgánica 15/1999 cumple las exigencias derivadas del principio de tipicidad, a juicio de esta Sala, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. En efecto, el tipo aplicable considera infracción grave "tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley", por tanto, se está describiendo una conducta –el tratamiento automatizado de datos personales o su uso posterior- que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la Ley Orgánica. Ahora bien, estos principios no son de aquellos que deben inferirse de dicha regulación legal, sino que aparecen claramente determinados y relacionados en el título II de la Ley, concretamente, por lo que ahora interesa, en el artículo 6 se recoge un principio que resulta elemental en la materia, que es la necesidad de consentimiento del afectado para que puedan tratarse automatizada mente datos de carácter personal. Por tanto, la conducta ilícita por la que se sanciona a la parte recurrente como responsable del tratamiento consiste en usar datos sin consentimiento de los titulares de los mismos, realizando envíos publicitarios."*

[37] Resolución: R/00215/2006, recaída en el Procedimiento sancionador N.º: PS/00093/2005, instruido por la AEPD.

Oñati Socio-Legal Series, v. 1, n. 8 (2011)
ISSN: 2079-5971

obtuvo. Se limita a manifestar, sin probarlo, que los datos de los colegiados que obran en el citado fichero proceden de fuentes accesibles al público, incluyendo dentro de éstas los directorios de los centros de trabajo de los médicos…"[38].

6. Conclusiones

El Derecho a la Protección de Datos, se configura como un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos de las personas mayores. Este Derecho fundamental, recogido en el art. 18.4 CE es, de acuerdo con el Tribunal Constitucional, en sí mismo "*un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".* De ahí la importancia de su estudio y, en especial, la incidencia en los derechos de las personas mayores y las consecuencias que el desconocimiento del mismo puede suponer.

La LOPD y su reglamento de desarrollo, junto con la normativa autonómica existente, regulan este Derecho. La citada normativa, se aplica a los datos de carácter personal registrados en soporte físico que los haga susceptible de tratamiento -tanto en soporte papel como informático- y, a todo uso posterior, que realicen los sectores público y privado. Se entiende por dato de carácter personal *"Cualquier información concerniente a personas físicas identificadas o identificables"* de ahí que se comprenda *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"* correspondiente a las personas mayores.

Los datos personales que se recopilen de las personas de la Tercera Edad y se introduzcan en ficheros de datos deben cumplir con la legalidad vigente y en consecuencia corresponde, entre otras cuestiones, que los ficheros estén inscriptos en las Agencias de Protección de Datos correspondiente y tener un Responsable del fichero o tratamiento. El responsable será el encargado de verificar el cumplimiento de la LOPD durante la existencia del fichero y de velar, especialmente, porque todos los datos introducidos en el fichero, por tanto los de las personas mayores, cuenten con consentimiento del titular del dato, definido como "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*". De esta forma, el titular de los datos cuenta con un poder de disposición y de control sobre los datos de manera que lo faculta a decidir qué datos va a proporcionar a un tercero o cuáles puede un tercero recabar. Asimismo le permite conocer quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión. Para que dicho consentimiento sea válido el mismo debe ser informado por tanto corresponde al responsable facilitar dicha información.

No obstante lo expresado anteriormente, la LOPD contiene algunas excepciones en las que el consentimiento no es necesario. En efecto, se trata de los supuestos en los que una Ley así lo autorice; cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado y cuando los datos figuren en fuentes accesibles al público y su tratamiento sea 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.

Si bien todos los datos personales quedan protegidos por la LOPD, algunos datos encuentran especial protección y requieren para su tratamiento el cumplimiento de unos requisitos concretos, tales como consentimiento expreso y por escrito,

[38] Resolución R/00362/2006, recaída en el procedimiento sancionador Nº PS/00344/2005, la AEPD.

inclusión exclusiva en ficheros públicos, prohibición de almacenarlos exclusivamente, etc. Se trata de los datos relativos a ideología, religión, afiliación sindical, creencias, origen racial, salud, vida sexual y los datos relativos a la comisión de infracciones penales o administrativas.

La dación de datos personales por parte de las personas mayores, bien sea a través del uso de las TIC o no, bien a instituciones –públicas o privadas-, bien a personas físicas, se debe efectuar con pleno conocimiento de la normativa sobre Protección de Datos. El desconocimiento de este derecho, tanto por la persona mayor como por aquellos que les apoyan, acompañan, asisten o representan puede causar perjuicios importantes a la dignidad, libertad y ejercicio de derechos. Esta situación puede ser aún más grave en aquellas personas mayores que se encuentran en situación de dependencia. En efecto, en estos casos, las residencias o los centros asistenciales que prestan auxilio a las personas mayores en situación de dependencia incorporan los datos a la Historia social, expediente donde se registran exhaustivamente los datos personales de los usuarios -familiares, sanitario, de vivienda, laborales, económicos, etc.- y que permite a los trabajadores sociales describir la situación de las personas que reciben los servicios. La mencionada historia social tiene que cumplir con la LOPD, lo que supone que sólo se puede incluir los datos facilitados por el titular del dato, salvo que se encuentre en algunas de las excepciones contempladas por la LOPD tales como que exista representante legal, que una Ley permita facilitar dichos datos a otra persona, que se recojan para el ejercicio de funciones propias de las administraciones públicas o que persiga proteger un interés vital de la persona mayor, entre otros. La historia social, sólo debe estar activa aquel tiempo que sea necesario para la prestación del servicio o, en su caso, transcurrido el plazo legal de cinco años debe ser cancelada.

A la historia social, sólo pueden acceder aquellas personas autorizadas y sólo a los datos que resulten necesarios para la gestión del servicio que desarrollan. Igualmente, en la citada historia sólo se pueden incluir los datos personales que sean pertinentes, adecuados y no excesivos para la finalidad del fichero. En los supuestos de que el dato sea especialmente protegidos, supuesto del dato religioso, se debe valorar por parte del responsable la adecuación de su inclusión en la historia social.

El acceso a los datos contenidos en la historia social es también un aspecto importante a destacar, dado que sólo se pueden comunicar a otras personas en los supuestos en los que exista previo consentimiento del titular de los datos o cuando una Ley así lo establezca. Esta última excepción permite ceder los datos a distintos órganos o instituciones, tales como los Órganos jurisdiccionales, al Ministerio Fiscal, las Fuerzas y Cuerpos de Seguridad del Estado, entre otros. En cualquier caso, siempre es posible la comunicación cuando el dato se encuentre disociado.

La protección que la LOPD le otorga al dato de carácter personal se extiende también a las medidas técnicas y organizativas que se deben adoptar para evitar que los datos puedan ser apropiados por terceros no autorizados. Se trata de las medidas de seguridad, medidas que dependiendo del tipo de datos que el fichero contenga, serán básicas, medias o altas. La historia social, al ser un fichero de datos, debe contar con estas medidas.

El secreto profesional, exigido a todos los profesionales que accedan a la historia social o fichero de datos, complementa la obligación del responsable de custodia de los datos, en tanto que el secreto obliga a guardar silencio sobre los datos que las personas conozcan del fichero, obligación que subsiste aún después de finalizada las relaciones con el titular del dato.

La teleasistencia es otro de los servicios que se ofrecen a las personas mayores en situación de dependencia y su prestación también se debe sujetar a la LOPD. De esta forma, todos los datos facilitados por la persona mayor para recibir este servicio se deben recoger, tratar y custodiar con pleno cumplimiento de la

normativa sobre protección de datos. En este caso, un dato peculiar es la voz de la persona mayor que se recoge y trata y que es un dato de carácter personal.

La peculiaridad de este servicio en relación con la aplicación del Derecho a la protección de datos la encontramos en los supuestos en los que se acude a solventar una emergencia de una persona mayor, dado que en estos casos, se protege un interés legítimo del afectado para la prestación sanitaria correspondiente y, por ello, la LOPD permite que el tratamiento de los datos no precise contar con el consentimiento del titular.

Igualmente, todas las personas mayores cuentan con una historia clínica, historia donde se contienen los datos de salud y cuya regulación se recoge en la LBrAP y, en las distintas normativas autonómicas que la complementan. La historia clínica tiene como fin principal facilitar la asistencia sanitaria y es un instrumento necesario para garantizar una atención adecuada al paciente. Se compone de distintos documentos y la LBrAP refuerza y remarca el reconocimiento del derecho de toda persona a que se respete el carácter confidencial de los datos referentes a su salud; confidencialidad que se completa con el secreto profesional que deben guardar todos los profesionales que accedan a la misma. La historia clínica también se encuentra sujeta a la LOPD, norma que define al dato de salud como un dato especialmente protegido y a la historia clínica como un fichero de datos que debe tener un responsable. Al responsable le corresponde garantizar que la historia contenga de forma clara, precisa, detallada y ordenada todos los datos relativos a la salud de un paciente, aplicar las medidas de seguridad correspondientes y conservar la documentación que se integra en la historia hasta cinco años como mínimo desde la fecha de alta de cada proceso asistencial, plazo que puede ser modificado en algunos casos por la normativa autonómica.

El acceso a las historia clínicas debe estar regulado para que sólo aquellas personas que estén autorizadas sean las que conozcan el dato. Así los profesionales, personal sanitario y administrativo, personal de inspección, evaluación, acreditación, etc. Un supuesto muy especial en el acceso a los datos es cuando los familiares de una persona mayor fallecida quieren acceder a la misma. En este caso, dado que los datos de las personas fallecidas no se encuentran dentro del ámbito de aplicación de la LODP ésta no es aplicable. Sin embargo, la LBrAP establece que se facilitará el acceso a la historia a los familiares de los pacientes fallecidos o personas vinculadas a él, salvo que el fallecido lo haya prohibido expresamente o que afecte a la intimidad del fallecido, a las anotaciones subjetivas de los profesionales y aquellas que perjudiquen a terceros. Igualmente, la LBrAP permite acceder a dichas historias cuando la persona justifique un riesgo para su salud, supuesto en el cual el acceso se verá limitado a los datos pertinentes.

Las personas mayores también se encuentran expuestas a la captación de su imagen –considerada dato de carácter personal- por medio de cámaras de video-vigilancia, cámaras que normalmente se suelen encontrar colocadas en los centros de cuidados, residencias, centros hospitalarios, centros asistenciales, centros comerciales, etc. Incluso, si residen en su domicilio, cuentan con un videoportero o también con sistemas de videovigilancia. La regulación de estos sistemas es peculiar y el consentimiento e información se produce por medio de un cartel informativo que debe colocarse en las entradas de los edificios. En principio la videovigilancia no puede captar imágenes de las vías públicas, lugar que se rige por la Ley Orgánica 4/1997, de 4 de agosto, de videovigilancia de las Fuerzas y Cuerpos de Seguridad del Estado y que otorga competencia exclusiva a las citadas Fuerzas. Tampoco las cámaras se pueden localizar en cualquier sitio, no pueden, como hemos visto, obtener imágenes de vías públicas o en lugares que sean lesivos para la dignidad personal, como habitaciones, baños, etc. Las imágenes captadas por las cámaras sólo se pueden ver por personas autorizadas y en lugares cerrados pudiéndose conservar las imágenes por un plazo máximo de un mes. Si una persona mayor quisiera acceder a sus datos debe solicitar el acceso al responsable

del fichero siempre que sea dentro del plazo de conservación y a quien corresponde hacer efectivo dicho derecho de acceso. Finalmente, en relación con los videoporteros tan sólo destacar que, en principio, si no graban se encuentran fuera del ámbito de aplicación de la LOPD, dado que su finalidad es verificar la identidad de las personas que llaman al timbre, y esta finalidad es considerada que pertenece al ámbito doméstico o personal. Si por el contrario, el videoportero graba o reproduce las imágenes captadas la LOPD es plenamente aplicable.

Por último, es preciso indicar que casi todas las personas mayores tienen en su domicilio un teléfono fijo, supuesto este último en el que sus datos personales se encontrarán recogidos en un repertorio telefónico o, en algunas de las denominadas, "Fuentes accesibles al público". En estos supuestos, el régimen de protección de datos difiere de los casos antes estudiados dado que cualquier persona puede acceder a los mismos sin consentimiento del titular del dato. Esto es así porque el procedimiento de inclusión en dichas Fuentes accesibles con carácter previo se encarga de solicitar al titular del dato el consentimiento. No obstante, es preciso indicar, que el hecho de que el dato figure en las citadas fuentes no supone que cualquiera pueda apropiarse del dato e incluirlo en un fichero sin más. Por el contrario, la propia LOPD, exige que el responsable del tratamiento del fichero donde se introduzca el dato tenga un interés legítimo para su tratamiento y no vulnere los derechos y libertades fundamentales del interesado.

En todos los casos antes descritos de tratamiento de datos si, el responsable del fichero, no cumple lo dispuesto por la LOPD será objeto de sanción por las infracciones que cometa por parte de las Agencias de protección de datos correspondiente. Estas infracciones pueden ser leves, graves o muy graves y si recaen sobre sujetos privados la multa que corresponde pagar será distinta según el tipo de infracción que la Agencia compruebe que ha cometido. Si, por el contrario el sujeto que comete la infracción es una persona pública, las Agencias verificarán la infracción cometida y una vez sancionada se comunica al Defensor del Pueblo a efectos de que éste incluya a la institución infractora del Derecho fundamental en su memoria.

7. Bibliografía

Agencia de Protección de Datos de la Comunidad de Madrid, 2008. *Protección de datos personales para Servicios Sanitarios Públicos*. Madrid: Thomson: Cívitas.

Agencia Española de Protección de Datos, 2009. *Guía de videovigilancia* [en línea]. Madrid: Agencia Española de Protección de Datos. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf [Acceso 28 noviembre 2011].

Agencia Española de Protección de Datos, 2010. *Guía de seguridad de datos, 2010* [en línea]. Madrid: Agencia Española de Protección de Datos. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf [Acceso 28 noviembre 2011].

Cáliz Cáliz, R., et al., 2009. *El Derecho a la protección de Datos en la Historia Clínica y la Receta Electrónica*. Pamplona: Aranzadi.

Dabove Caramuto, María Isolina, 2002. Consentimiento informado y Derecho de la ancianidad: investigación, tratamientos terapéuticos en Geriátricos. *En*: *Bioética: entre utopías y desarraigos, Libro homenaje a la profesora Dra. Gladys J. Mackinson*. Buenos Aires: Ad Hoc, 2002, 489-495.

Dabove Caramuto, María Isolina, 2005. *Los derechos de los ancianos*. Buenos Aires, Madrid: Ciudad Argentina.

Dabove Caramuto, María Isolina, 2006. *Derecho de la Ancianidad. Perspectiva Interdisciplinaria*. Prólogo a cargo de la Dra. Mónica Roqué. Rosario: Juris.

Davara Rodríguez, M.A., 1998. *La protección de datos en Europa: principios, derechos y procedimiento*. Madrid: Grupo Asnef Equifax.

Davara Rodríguez, M.A., 2008. *Manual de Derecho Informático*. Pamplona: Aranzadi.

De la Serna Bilbao, M.N., 1997. La agencia de Protección de datos española: con especial referencia a su característica de independiente. *Revista Actualidad Informática Aranzadi*, 22, 1 y 10-15.

De la Serna Bilbao, M.N., 2010. Comentario al artículo 3.j) de la LOPD. *En*: Antonio Troncoso Reigada, dir. *Comentario a la Ley Orgánica de protección de datos de carácter personal*. Madrid: Thomson Civitas.

De la Serna Bilbao, M.N., 2010. Las telecomunicaciones y la protección de datos: las guías, otros directorios telefónicos y la prestación del servicio de información de teléfonos a los usuarios. *En*: Comentarios a la Ley de Tecnologías de la Información y las comunicaciones –TIC–. Bogotá: Universidad Externado Colombia.

Fonseca Ferrandis, F., 2010. Comentario al artículo 2 de la LOPD. *En*: Antonio Troncoso Reigada, dir. *Comentario a la Ley Orgánica de protección de datos de carácter personal*. Madrid: Thomson Civitas.

Gómez-Juárez Sidera, I., 2009. *Aprenda a proteger sus datos: Guía de protección de datos para personas mayores*, 2009 [en línea].Madrid: ASIMELEC con la colaboración de la Agencia Estatal de Protección de Datos. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_mayores_05_2009.pdf [Acceso 28 noviembre 2011].

Lucas Murillo de la Cueva, P., Piñar Mañas, J. L., 2009. *El Derecho a la Autodeterminación informativa*. Madrid: Fundación Coloquio Jurídico Europeo.

Martínez Martínez, R, 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson/Civitas.

Palomar Olmeda, A. y González-Espejo, P., dirs., 2009. *Comentario al reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, Madrid: Thomson/Cívitas.

Pérez Luño, A., 1989. Los Derechos Humanos en la sociedad tecnológica. En: Mario G. Losano, Antonio Enrique Pérez Luño, María Fernanda Guerrero Mateus. *Libertad informática y leyes de protección de datos personales*. Madrid: Centro de Estudios Constitucionales.

Rallo Lombarte, A. y Martínez Martínez, R., coords. 2010. *Derecho y redes sociales*. Madrid: Civitas/Thomson.

Romeo Casabona, C., 2004. La protección penal del secreto profesional y laboral en el Derecho penal. *En*: *Estudios penales en recuerdo del Profesor Ruiz Antón*. Valencia: Tirant lo Blanch.

Sánchez Caro, J. y Abellán F., 2003. *Derechos y Deberes de los pacientes (Ley 41/2003, de 14 de noviembre, consentimiento informado, historia clínica, intimidad e instrucciones previas)*. Madrid: Fundación Salud 2000.

Téllez Aguilera A., 2002. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores.* Madrid: Edisofer.

Troncoso Reigada, A., 2010a. La *protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Troncoso Reigada, A., dir., 2010b. *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Madrid: Thomson/Civitas.

Vizcaíno Calderón, M., 2001. *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal*. Madrid: Civitas.