UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA : EVOLUCIÓN NORMATIVA Y CRITERIOS DE APLICACIÓN

MEMORIA PARA OPTAR AL GRADO DE DOCTOR
PRESENTADA POR

Emilia Zaballos Pulido

Bajo la dirección del doctor

Emilio Suñé Llinás

MADRID, 2013

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA

EVOLUCIÓN NORMATIVA Y CRITERIOS DE APLICACIÓN

TESIS DOCTORAL PRESENTADA POR

EMILIA ZABALLOS PULIDO

DIRECTOR DE TESIS: EMILIO SUÑÉ LLINAS

MADRID, 2013

ÍNDICE

Índice de contenido

ABSTRACT

The Spanish Constitution states in its Article 18 the right to honour, to personal and family privacy and self-image; the inviolability of the home and the secrecy of communications. However, Article 18 also safeguards, in its fourth paragraph, another fundamental right, which is not less important than the ones mentioned above: the limitation of the use of computer technology to ensure the honour and personal and family privacy of citizens and the full exercise of their rights. Article 18.4 of the Spanish Constitution guarantees, ultimately the fundamental right to personal data protection that ensures the control over personal data as well as its use and destination, with the ultimate aim to avoid its use as a means to undermine citizens´ dignity and their rights.

The development of this constitutional provision, in our domestic legislation, was conducted by means of the Organic Law 5/1992, from October 29, for the regulation of the automated processing of personal data (LORTAD). This standard was replaced by the Organic Law 15/1999, from December 13, bypersonal data protection, also known as LOPD. In 1999 the LOPD was published and a few months prior to that the Regulations of Security Measures Act was promulgated through the Article 9 of the LORTAD. The LORTAD established the necessity to regulate, in a statutory form, the requirements and conditions, which automated filing systems and the individuals who intervene in the process of dealing with personal data should have. It was not until the year 2007 that the Spanish legislator promulgated the Regulations of Development of the LOPD through the Royal Decree 1720/2007.

Our legislation, in respect to personal data protection, needs a change. This change has to be in accordance with the new needs caused by the unstoppable advance intechnology. But it also, undoubtedly, needs to rely on the expertise of these fifteen years, since this experience is going to be vital. Being able to learn from the mistakes of the past will lead us to having cutting edge legislation onpersonal data

protection, not only in accordance with the new technological world around us, but also with the demands that are going to be imposed by the European Union.

In fact, while we are reading these lines, the European Union is preparing a new regulation on data protection. Yes, a regulation and not a directive, which means an even bigger obligation. We cannot forget that European Union regulations have a general reach and a direct efficacy, which implies that they are directly applicable in all the EU nations by any given authority or individual without the need of a judicial norm of internal or national origin to reach its full efficacy. Regulations are different from directives, though they also have a general reach. However, they set objectives and binding deadlines but leave it up to the states to choose the most suitable means.

As we can see we are experiencing a critical moment. Personal data protection needs to be reviewed from the base as a means to adapt to the new future that the new technological challenges lay out in front of us when facing the correct protection of fundamental rights that are at stake. For this reason it is necessary to have a study whichwould expose with clarity all the experience gained during the 15 years of legislative development articulated around personal data protection. Or rather thirty-four years, if we take into account the entry into force of the Spanish Constitution, a key moment in our democracy and to which we should be thankful for its visionary and innovative spirit, at least in the Article 18.4 of this text.

This study therefore aims to bring together and study the experience which has been provided to us by the Spanish legislation in the field of personal data protection. An experience that will be undoubtedly useful in the near future where *information technology laws* will have changed. If during those years legislation was based on completely centralised computing and personal computers and the paper medium were the main focal point, nowadays we need to see that information, personal data and information technology itself are completely decentralised.

Therefore, we are going to focus our vision on the following content:

- **The fundamental right to personal data protection**: Where we will analyze the nature and content of the right to privacy and the definition of concepts such as privacy and where we will also review the national, European and international legislation, ever so more important in the subject matter of our study.
- **Principles of data protection**: an analysis of the areas covered by the legal regime of protection and specifically, which is the area covered by the LOPD. We will look at what is essential to determine the scope of application of the LOPD. This will lead to being faced with personal data forming part, or readiness to be a part of a personal data file and the treatment that they undergo. To do this, we will focus on the analysis of three concepts: personal data, file and treatment, and later detail what is the subjective scope of application, that is, that individuals are subject to the obligations contained in the LOPD and what are the special cases that we need to know to carry out a proper implementation of the regulations.
- **ARCO rights**: Here we will analyze the rights of access, rectification, cancellation and opposition, also known as ARCO rights or the rights of people or of the person concerned as a set of guarantees that the Spanish legislation in the field of protection of data sets out for the holders of the given rights so that they may have control over their possible useby public and private entities.
- **Security**: The principle of security of data assigns the individuals responsible for the file the obligation to take measures of technical and organizational nature necessary to ensure the security of personal data and prevent its alteration, loss, treatment or unauthorized access. We will look, at this point, at how this principle is configured as one of the pillars of the fundamental right to personal data protection by focusing on the analysis and

study of the regulation concerning the principle of security, from both the European level, as wellas from the point of view of national legislation.

- **The Regulation of the development of the LOPD**: At this point, we will analyze the new Regulation of the Development of the LOPD, adopted by the Royal Decree 1720/2007, from 19 January 2008, and that comes in response to the need for a supplemental text for the Data Protection Act to allow the individuals responsible for treatment to have a frame of reference for the implementation of the security measures.

The analysis and the study of this work have been carried out, based on an **extensive<u>Bibliography</u>**, part of which is listed below.

ALMUZARA ALMAIDA, C. (Coord.) (2005). Estudio Práctico sobre la protección de datos de carácter personal. Editorial Lex Nova. Valladolid.

APARICIO SALOM, J. (2000). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Editorial Aranzadi. Elcano (Navarra).

CARRERAS SERRA, L. (2003). Derecho Español de la Información. UOC. UniversitatOberta de Catalunya.

CONDE ORTIZ, C. (2005). La protección de datos personales. Dykinson.

DAVARA RODRÍGUEZ, M. (2006). Manual de Derecho Informático 8ª Edición. Thomson Aranzadi.

DEL PESO NAVARRO, Emilio (2000). Ley de Protección de Datos: la nueva LORTAD. Editorial Díaz de Santos. Madrid.

GÓMEZ NAVAJAS, J. (2005). La protección de datos personales. Un análisis desde la perspectiva del derecho penal. Thomson Civitas. Madrid.

HERRAN ORTIZ, A. (2002). El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales. Dykinson. Madrid.

MAESTRE RODRÍGUEZ, J.A. (2003). La intimidad: El derecho de autodeterminación personal. En Nuevas Tecnologías de la Información y Derechos Humanos. Cedecs.

MARZO PORTERA, A. y MACHO-QUEVEDO, A. (2004): La Auditoría de Seguridad en la Protección de Datos de Carácter Personal. Ediciones Experiencia. Barcelona.

MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto (2000). La cesión o comunicación de datos de carácter personal. Editorial Thompson Civitas. gencia de Protección de Datos de la Comunidad de Madrid. Madrid.

SUÑÉ LLINAS, E. (1999). Tratado de derecho informático. Introducción y protección de datos personales (Volumen I; 2ª edición). Madrid: Servicio de publicaciones de la facultad de derecho. Universidad Complutense de Madrid.

ULL PONT, E. (2003). Derecho Público de la Informática. Protección de Datos de Carácter Personal. 2ª edición actualizada, UNED Ediciones. Madrid.

JUSTIFICACIÓN

La Constitución Española de 1978, publicada en el Boletín Oficial del Estado de 29 de diciembre de 1978, establece en su artículo 18 el Derecho al honor, a la intimidad personal y familiar y a la propia imagen; la inviolabilidad del domicilio y el secreto de las comunicaciones.

Estos son los derechos fundamentales y libertades públicas más conocidos. Sin embargo, el artículo 18 también guarda, en su cuarto apartado, otro derecho fundamental no menos importante que los citados anteriormente. Nos referimos, por supuesto, a la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Nuestra Carta Magna fue una de las primeras constituciones europeas en introducir esta limitación del uso de la informática, algo sin duda, mérito de los legisladores de la época que fueron capaces de darse cuenta de los peligros que, para el honor y la intimidad personal y familiar de los ciudadanos, esta *nueva* tecnología podía suponer y tomaron como ejemplo la Constitución Portuguesa, sólo dos años anterior a nuestro texto constitucional, para incorporar a nuestro derecho, esta importante limitación.

Poniéndonos en contexto, la década de los setenta se caracteriza por la madurez tecnológica que suponían las conocidas como *minicomputadoras*, también conocidas como computadoras de tercera generación, y que dio paso, a inicios de los años setenta a la llegada de las *microcomputadoras personales* o computadoras de cuarta generación, caracterizadas por incorporar un microprocesador y sobre todos, por constituir una herramienta al alcance del gran público, ya que hasta ese momento esta tecnología sólo se encontraba en manos de un grupo muy selecto.

La posibilidad de que el gran público, es decir, los ciudadanos dispusiesen de una herramienta con una gran capacidad de cálculo y de almacenamiento de información fue la clave para que nuestros legisladores incluyesen en el texto constitucional esta vaga referencia a que 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. Una vaga referencia, sí, pero sin duda una gran previsión ya que el futuro que estaba por llegar era insospechado. No podemos pasar por alto que en los años 70 se utilizaba la informática como una herramienta cotidiana, generando un tratamiento mecánico de la información.

Tal y como expresa la Profesora Cuadrado Gamarra[1], *desde los inicios de la informática, se ha producido una interacción entre ella y el Derecho.*

Sólo tres años después de la entrada en vigor del texto constitucional, en 1981, nace la quinta generación de computadoras, también conocido como PC u ordenador personal y que ya incorporaba novedosos avances como la incorporación, en sus sistemas, del lenguaje natural, la inteligencia artificial así como amplias posibilidades de interconexión.

En un primer momento, se consideró el derecho establecido en el apartado cuarto del artículo 18 de la Constitución Española, como una especialización del derecho a la intimidad, pero nuestro Tribunal Constitucional ha interpretado que se trata de un derecho independiente, aunque obviamente estrechamente relacionado con aquél tal y como se puede apreciar en diversas sentencias de nuestro Alto Tribunal:

«Dispone el art. 18.4 C.E. que "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". De este modo, nuestra Constitución ha incorporado una ***nueva garantía constitucional****, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática"»*[2].

Asimismo, y en esta mista sentencia citada anteriormente, también señaló la vinculación directa de este derecho para los poderes públicos sin necesidad de desarrollo normativo:

[1] CUADRADO GAMARRA, N. (2005). *Capacidad jurídica y derechos subjetivos en relación con las Nuevas Tecnologías.* En La capacidad Jurídica. Madrid: Dykinson. Pág. 173

2 Tribunal Constitucional, Sala Primera, Sentencia 254/1993 de 20 Julio de 1993, recurso 1827/1990.

«El primer problema que este derecho suscita es el de la ausencia, hasta un momento reciente, en todo caso posterior a los hechos que dan lugar a la presente demanda, de un desarrollo legislativo del mismo. Ahora bien, a esa ausencia de legislación no se pueden enlazar las desmesuradas consecuencias que postula el Abogado del Estado. Aun en la hipótesis de que un derecho constitucional requiera una interpositio legislatoris para su desarrollo y plena eficacia, nuestra jurisprudencia niega que su reconocimiento por la Constitución no tenga otra consecuencia que la de establecer un mandato dirigido al legislador sin virtualidad para amparar por sí mismo pretensiones individuales, de modo que solo sea exigible cuando el legislador lo haya desarrollado. Los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos. Este principio general de aplicabilidad inmediata no sufre más excepciones que las que imponga la propia Constitución, expresamente o bien por la naturaleza misma de la norma (STC 15/1982, fundamento jurídico 8.).

Es cierto que, como señalamos en esa misma Sentencia, cuando se opera con una «reserva de configuración legal» es posible que el mandato constitucional no tenga, hasta que la regulación se produzca, más que un mínimo contenido, que ha de verse desarrollado y completado por el legislador. Pero de aquí no puede deducirse sin más (como hace el Abogado del Estado), que los derechos a obtener información ejercitados por el demandante de amparo no forman parte del contenido mínimo que consagra el art. 18 C.E. con eficacia directa, y que debe ser protegido por todos los poderes públicos y, en último término, por este Tribunal a través del recurso de amparo (art. 53 C.E.)».

Por tanto, el artículo 18.4 de la Constitución Española que que garantiza, en última instancia es un derecho fundamental a la protección de datos de carácter personal que garantiza a las personas el control sobre sus datos personales así como su uso y destino, con la finalidad última de evitar el uso de los mismos como un medio para menoscabar su dignidad y sus derechos.

El desarrollo de este precepto constitucional, en nuestra legislación interna, se llevo a cabo por medio de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, también conocida como LORTAD en cuya exposición de motivos encontramos sus objetivos principales:

«La Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática.

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que

se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos.

Los más diversos datos -sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado dinero plástico, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner solo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor una frontera que sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley».

Con la entrada en vigor de la LORTAD podemos decir, sin miedo a equivocarnos, que es el momento de la historia legislativa española en el cual se garantiza la protección de los datos de carácter personal. Bien es cierto, que la LORTAD es víctima de su tiempo y, por tanto, sólo garantiza la protección de los datos personales almacenados en soportes automatizados, dejando sin protección a todos aquellos datos de carácter personal tratados en soportes no automatizados o soporte papel. Pero dicha circunstancia sólo es consecuencia del atroz miedo que se tenía al uso de la informática, sobre todo en cuanto a su capacidad de almacenamiento y de tratamiento de la información.

La LORTAD, como tal, sólo estuvo vigente 7 años ya que fue sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, también conocida como LOPD, fruto de la imposición europea que obligó al Estado español a transponer a su derecho interno 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, como medio para *limar* los obstáculos para el ejercicio de actividades económicas a escala comunitaria, falsear la competencia así como impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario.

Y decimos que la LORTAD sólo estuvo vigente, como tal, 7 años porque en realidad podemos decir que la LOPD es la *hija aventajada* de la LORTAD ya que en esencia es un *calco* bastante fiel de todos y cada uno de los preceptos enumerados por la LORTAD hasta tal punto que casi podía pensarse que ambas normas son idénticas sino fuese por la introducción, en la LOPD, de algunas figuras establecidas e impuestas por la Directiva 95/46/CE como puede ser, por ejemplo, la figura del encargado del tratamiento.

Tal es así que en 1999, fecha en la que vio la luz la LOPD, se promulgó, con unos meses de antelación el Reglamento de Medidas de Seguridad establecido por el artículo 9 de la LORTAD que establecía la necesidad de regular, de forma reglamentaria, los requisitos y condiciones que debían reunir los ficheros automatizados y las personas que interviniesen en el tratamiento automatizado de los datos de carácter personal. En este sentido, el Reglamento de Medidas de Seguridad fue publicado en el Boletín Oficial del Estado, a través del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal y que ha convivido con la LOPD durante más de ocho años.

No fue hasta el año 2007, cuando el legislador español promulgó el Reglamento de Desarrollo de la LOPD a través del Real Decreto 1720/2007 y nace con la intención no sólo de sustituir a un Reglamento de Medidas de Seguridad, ideado para una Ley que pretendía salvaguardar a los ciudadanos de los riesgos de una informática distribuida sino también como medio de desarrollar y regular algunos puntos en los que la experiencia de más de 15 años de regulación en materia de protección de datos de carácter personal, hacían necesario un mayor punto de concreción.

El presente estudio nace, por tanto, con la premisa de aglutinar y estudiar la experiencia que la legislación española, en materia de protección de datos de carácter personal nos ha proporcionado. Una experiencia que, sin duda, nos será útil en nuestro futuro más cercano en donde las *leyes de la informática* han cambiado. Si durante estos años la legislación se basaba en una informática totalmente centralizada y donde los ordenadores personales y el soporte papel eran su foco de atención, hoy en día debemos partir de la premisa de que la información, los datos personales y la informática en sí misma se encuentran totalmente descentralizadas.

La informática y el tratamiento de la información ya no se basan en ordenadores personales con una posibilidad de interconexión, denominémosla, *limitada.* Al contrario, hoy en día, el máximo exponente de la informática y las Nuevas Tecnologías es Internet, la red de redes y sus connatural posibilidad de conexión.

Internet, unida a las nuevas tecnologías en materia de telecomunicaciones hacen posible que naveguemos a través de dispositivos móviles tan dispares como los *smartphones*, *las tablets*, los ordenadores portátiles, etcétera. A este cambio radical de concepto se une el denominado cambio social conocido como Web 2.0 en el que los usuarios se convierten en el motor principal de Internet a la cual alimentan con un sinfín de contenidos a través de las redes sociales, los foros o los chats por citar sólo unos ejemplos.

Asimismo los mecanismos informáticos han cambiado y hoy en día se tiende a que la información no radique en discos duros o servidores perfectamente controlados y tasados sino que la computación en nube o *cloud computing* abre las puertas al tratamiento de la información y, por tanto, de los datos personales a un nuevo mundo. Un mundo expuesto a una gran variedad de riesgos que la legislación no puede obviar y dejar de lado si realmente se pretende garantizar la intimidad personal y familiar de los ciudadanos así como una correcta y legal protección de sus datos de carácter personal.

Nuestra legislación, en materia de protección de datos de carácter personal, demanda un cambio. Un cambio acorde a las nuevas necesidades provocadas por el avance imparable de la tecnología. Pero este cambio necesita, sin duda alguna, apoyarse en la experiencia de estos quince años, ya que dicha experiencia va a ser vital. Aprender de los errores del

pasado nos llevará a disponer de una legislación puntera en materia de protección de datos de carácter personal, no sólo acorde al nuevo mundo tecnológico que nos rodea sino también acorde a las exigencias que desde la Unión Europea se nos van a imponer.

De hecho, mientras leemos esta líneas desde la Unión Europea se está preparando un nuevo Reglamento en materia de protección de datos. Sí, un Reglamento y no una Directiva lo cual si cabe impone una mayor carga obligatoria, ya que no debemos olvidar que los Reglamentos de carácter europeo tienen alcance general y eficacia directa lo cual implica que son directamente aplicables en todos los Estados de la Unión por cualquier autoridad o particular, sin que sea precisa ninguna norma jurídica de origen interno o nacional que la transponga para completar su eficacia plena y que difieren de las Directivas en que éstas, si bien también disponen de alcance general, las últimas fijan unos objetivos y plazos vinculantes, dejando libertad a los Estados para escoger los medios adecuados.

Hablamos, por tanto, de un giro copernicano a nivel europeo, en materia de protección de datos de carácter personal. Hablamos por tanto, de una norma totalmente homogénea, a nivel europeo y de la cual ya tenemos un borrador[3] o *propuesta,* denominado Reglamento General de Protección de Datos basado en el siguiente contexto:

«La presente exposición de motivos presenta en detalle el nuevo marco jurídico propuesto para la protección de los datos personales en la UE, como se establece en la Comunicación COM (2012) 9 final. El nuevo marco jurídico propuesto consta de dos propuestas legislativas:

- una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), y

– una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre

3 Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

circulación de estos datos;

La presente exposición de motivos se refiere a la propuesta legislativa de Reglamento general de protección de datos.

La piedra angular de la legislación vigente de la UE en materia de protección de datos, la Directiva 95/46/CE, fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros. Se complementó mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

La rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social.

Generar confianza en el entorno en línea es esencial para el desarrollo económico. La falta de confianza hace que los consumidores vacilen a la hora de adquirir productos en línea y adoptar nuevos servicios, con lo que se corre el riesgo de que se ralentice el desarrollo de usos innovadores de las nuevas tecnologías. La protección de datos personales desempeña, por tanto, una función esencial en la Agenda Digital para Europa y más concretamente en la Estrategia Europa 2020.

El artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), introducido por el Tratado de Lisboa, establece el principio según el cual toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Además, con el artículo 16, apartado 2, del TFUE, el Tratado de Lisboa introdujo una base jurídica específica para la adopción de normas relativas a la protección de datos de carácter personal. El artículo 8 de la Carta de los Derechos Fundamentales de la UE consagra como derecho fundamental la protección de los datos de carácter personal.

El Consejo Europeo invitó a la Comisión a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas. En su resolución sobre el Programa de Estocolmo, el Parlamento Europeo acogió favorablemente un régimen general de protección de datos en la UE y, entre otras cosas, abogó por la revisión de la Decisión Marco. En su Plan de acción por el que se aplica el Programa de Estocolmo, la Comisión subrayó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplique de forma coherente en el contexto de todas las políticas de la UE.

En su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», la Comisión concluyó que la UE necesita una política más integradora y coherente en materia del derecho fundamental a la protección de los datos de carácter personal.

Si bien el marco jurídico actual sigue siendo adecuado por lo que respecta a sus objetivos y principios, no ha evitado, sin embargo, la fragmentación en cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea. Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas».

Como podemos observar no encontramos en un momento crítico. La protección de los datos de carácter personal necesita ser revisada desde la base como medio para adaptarse al nuevo futuro que los nuevos retos tecnológicos nos planteas de cara a una correcta protección de los derechos fundamentales que están en juego.

Por esta razón se hace necesario un trabajo en el que se exponga con claridad toda la experiencia adquirida durante los 15 años de desarrollo legislativo articulado en torno a la protección de los datos de carácter personal. Treinta y cuatro años si tenemos en cuenta la entrada en vigor de la Constitución Española, momento clave de nuestra democracia y a la

cual debemos agradecer su espíritu visionario e innovador al recoger en el apartado cuarto de su artículo 18 la ya conocida limitación de la informática para para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Gracias a este artículo y gracias a la tremenda visión de nuestros legisladores, al basarse en la Constitución Portuguesa, nos encontramos en disposición de afrontar los retos del futuro con una experiencia, extensa y rica, que nos permitirá, no caer en los errores del pasado y dotar a la protección de los datos de carácter personal, la regulación que se merece. Una regulación a la altura del resto de derechos fundamentales y libertades públicas promulgados en nuestra Carta Magna.

LOS DATOS DE CARÁCTER PERSONAL

I. INTRODUCCIÓN

Uno de los aspectos fundamentales para entender el origen y la evolución de la protección de los datos de carácter personal ha sido el crecimiento de todos los ámbitos relacionados con las Tecnologías de la Información y las Comunicaciones (TIC), que ha implicado la constante creación de productos y servicios cada vez más accesibles a los ciudadanos y que está impulsando la introducción de nuevas formas de trabajar, de relacionarse y, en general, de comunicarse.

Este desarrollo incluye la aparición de medios que permiten la gestión automatizada de la información, el tratamiento y el análisis discriminado de ingentes volúmenes de datos. La accesibilidad y capacidad de procesamiento de estos medios no han hecho sino incrementarse a lo largo de las últimas décadas[4]. En lo que afecta a la protección de los datos de carácter personal, la aplicación de estos medios a información concerniente a personas físicas, puede afectar directamente al ámbito de la intimidad de estas personas.

En la actualidad el acceso a todo tipo de bienes y servicios exige la entrega de datos personales, y las personas no siempre son conscientes de que este hecho va configurando un rastro de información que escapa a todo control. Información que puede ser sometida a tratamientos que permitan obtener información muy valiosa sobre aspectos concretos de la personalidad como gustos, intereses, hábitos de consumo, etc..

Proteger adecuadamente este ámbito exige delimitar cual es el contenido que está siendo afectado. La reflexión sobre este punto nos llevará a analizar la naturaleza y el contenido del derecho a la intimidad y la definición de conceptos como “privacidad”.

4 La llamada Ley de Moore, enunciada en 1965, puede resumirse como un principio que indica el incremento en la capacidad de los equipos sin que ello conlleve un aumento equivalente en el coste. Se ha venido cumpliendo hasta ahora. Conforme a la Ley de Moore cada dieciocho meses se duplica la potencia de los equipos, manteniéndose los costos, lo que ha derivado en una enorme potencia de proceso cada vez más accesible a todos.

1. Informática

La informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales.

El origen de las investigaciones sobre los tratamientos de información y la computación comienza alrededor de 1930[5], el término "informática", es atribuible al ingeniero francés Philippe Dreyfus que utilizó "*informatique"* por primera vez en 1962, como acrónimo de las palabras "*information"* y "*automatique"*.

Lo que hoy en día conocemos comúnmente como "informática" está conformado por muchas técnicas y áreas de conocimiento, que van desde la gestión de negocio, el almacenamiento de información, el control de procesos o las comunicaciones.

En lo relativo a la evolución de la informática a lo largo del siglo XX, puede afirmarse que ha tendido al diseño de técnicas y sistemas cada vez más compatibles, acompañadas del progresivo abaratamiento de los costes de los componentes y los equipos informáticos.

Estos dos han sido los factores clave en la aparición de la denominada "**Sociedad de la Información**", modelo en el que la Informática está presente de manera masiva en todos los ámbitos de la Sociedad, y muy especialmente en las actividades económicas así como en el propio tejido social.

Por otra parte, y como afirma Márquez Lobillo[6], no podemos afirmar que el proceso de informatización de la sociedad haya concluido, sino que probablemente nos encontremos en el inicio de modelos y formas de convivencia que podemos anticipar solo en parte:

"*El final de la década de los noventa y los albores del nuevo siglo son el punto de partida de una nueva etapa en el desarrollo de lo que será la verdadera sociedad de la información, del conocimiento, la cibersociedad... cuyo punto álgido se alcanzará, cuando la mayoría de los ciudadanos pueda acceder a cualquier tipo de información, con*

5 El matemático Howard Aiken, es considerado por algunos autores como el inventor del primer ordenador, entre 1937 y 1943, aunque en ese periodo fueron numerosos los avances en distintos campos relacionados

6 MÁRQUEZ LOBILLO P. (2004). *Empresarios y profesionales en la sociedad de información*. Edersa, 2004. Págs. 45 a 47

independencia del tiempo, del lugar en el que se encuentren o de la forma en la que la misma sea presentada.

Estamos en la era de los ordenadores portátiles, de la telefonía móvil, de la televisión por cable, del teletrabajo, la telemedicina o la teleeducación, la era de la conexión a redes que permiten entablar las más variadas modalidades de relaciones personales, asistenciales, comerciales..., al eliminarse las barreras espaciales y temporales.

La generalización social de los tradicionales medios de computación y comunicación y la incorporación de otros nuevos, permiten el acceso a mayor información, constituyendo los pilares necesarios para la madurez del nuevo escenario social al que nos enfrentamos.

La convergencia entre las tecnologías multimedia -información, comunicación y audiovisual- como elemento imprescindible para que el acceso a información de cualquier tipo, en cualquier lugar y en cualquier momento sea una realidad, pone realmente de relieve una (…) transformación considerable del mercado electrónico de la información, que da nacimiento a una verdadera sociedad de la información"

Hemos utilizado ya dos conceptos que son básicos para la materia que nos disponemos a estudiar: "Datos" e "Información". Conviene detenerse ahora un un instante para definir convenientemente estos dos conceptos así como otros que también interesan al objeto de la presente

- **Dato:** Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho.
- **Información:** Suma de los datos con sentido, relevancia y propósito
- **Conocimiento:** Capacidad de trasformar los datos y la información en acción. El conocimiento permite interconectar y aplicar los datos y la información.
- **Tratamiento de la Información:** Aplicación de técnicas o programas de forma sistemática sobre un conjunto de datos, con el objeto de obtener información o conocimientos que van más allá de los datos utilizados. En los casos en los que estos datos aluden a características de personas físicas es posible establecer pautas y relaciones que finalmente pueden configurar perfiles y permitir a aquellos que llevan a cabo el tratamiento, acceder a un

conocimiento sobre los titulares de los datos que indudablemente tiene un gran valor (económico, político, social), y que afecta a la esfera de su intimidad pudiendo ir más allá de la finalidad para la que los datos personales fueron originalmente facilitados.

2. La sociedad de la información

El crecimiento de los tratamientos de información, tanto en su número como en el volumen de datos implicados, está estrechamente relacionado con el desarrollo de lo que se ha venido a denominar "**Sociedad de la Información".**

Utilizamos el término "Sociedad de la Información" en cualquier contexto que tenga relación con las Tecnologías de la Información y las Comunicaciones, habiéndose finalmente convertido en un lugar común sin un significado concreto.

En el ámbito jurídico, su utilización ha sido consagrada a través de la UE, que lo ha utilizado profusamente en recomendaciones, informes y directivas sobre este tema. No obstante, su origen no es jurídico sino que aparece en el ámbito de la economía.

Surge sobre 1970 a raíz de un informe del instituto de prospectiva japonés JACUDI, en el que se hacía una especial referencia al valor económico de la información. Con posterioridad, el término fue haciéndose cada vez más conocido gracias a las aportaciones de otros autores, siendo uno de los primeros en utilizarlo a nivel teórico el economista austriaco Fritz Machlup. En la década de los setenta empezaba a hacerse evidente la importancia de la Información dentro del ámbito económico y se comenzaba a percibir un cambio en la forma de funcionamiento de las sociedades que derivó en un modelo que vendría a suceder a la Sociedad Industrial.

Los medios de generación de riqueza poco a poco se iban trasladando de los sectores industriales a los servicios y la mayor parte de los empleos ya no estaban asociados a las fábricas de productos tangibles, sino a la generación, almacenamiento y procesamiento de todo tipo de información. Aparecían las "*industrias sin chimenea*", basadas en un modelo económico en el que las TIC empezaban a ser el fundamento esencial del desarrollo.

En la década de los noventa, el desarrollo tecnológico propiciaba otro importante avance con la generalización de la informática, Internet y en general, de las TIC. De los años noventa datan informes económicos de algunos de los países líderes en la materia que atribuyen a las tecnologías de la Información la responsabilidad directa de que el crecimiento económico real aumentara en casi una cuarta parte. Se empezaba a hablar de la "**Nueva Economía**", término acuñado a finales de los años 90 para describir la evolución, en EEUU y otros países desarrollados, de una economía basada principalmente en el conocimiento, debido en parte a los nuevos progresos en tecnología y en parte a la globalización económica[7]. Fue utilizado por primera vez por el economista Brian Arthur en 1996 y popularizado en aquellos años por Kevin Nelly, editor de la revista "Wired".

A nivel mundial, el número de personas conectadas a Internet continuó aumentando progresivamente a un ritmo de crecimiento difícilmente previsible en los años anteriores. En 1996 se estimaba que existían 40 millones de personas conectadas a la red; sólo un año después eran 100 millones. En España, la evolución fue también espectacular. En 1995 eran sólo 45.000 las personas que hacían uso de la red, mientras que en 1997 contábamos con 8 millones de usuarios de ordenadores, un 10 por ciento más que en 1996; al mismo tiempo, el porcentaje de internautas era de 1,3 millones lo cual suponía un 78 por ciento de crecimiento con relación a 1996 mientras que el comercio electrónico crecía a un ritmo del 30 por ciento anual[8]. Y el proceso dista mucho de cerrarse, sino que seguirá creciendo. Los datos de consumo y las encuestas a usuarios de las TIC muestran, año a año, como se está propiciando en todos los ámbitos de la sociedad un cambio de comportamiento así como cultural profundo.

3. La UE y la Sociedad de la Información

En 1993, se publica el Informe Bangemann que surgía al calor de una iniciativa estadounidense publicada en septiembre del mismo año, titulada: *«The national*

7 En este contexto, las inversiones en Tecnologías de la Información pasaron a representar el 45% de las inversiones empresariales en bienes de equipo, mientras que en los años 60 esta inversión sólo representaba un 3% del total.

8 Boletín Oficial de las Cortes Generales (1999). *Informe de la Comisión Especial sobre redes informáticas del Senado*. Senado, número 812, 27 de diciembre.

information infraestructure: agenda for action».

El Consejo Europeo de Bruselas solicitó a la Comisión la elaboración de un informe sobre medidas específicas a seguir para la creación de infraestructuras de información en el ámbito de los Estados Miembros. El Informe propone un Plan de Acción que permita alcanzar en la UE la «Sociedad de de la Información» mediante la combinación de las fuerzas de los sectores público y privado. De la elaboración de dicho Plan se deduce que este futuro nuevo estadio de la Sociedad asentado en la Información no es una consecuencia automática de la revolución tecnológica, sino que debe fomentarse, en este caso, a nivel comunitario[9].

El Plan propuesto se centró en tres líneas:

- Evitar el rechazo que pueda tener el uso de las nuevas tecnologías entre sus destinatarios fomentando entre la población lo que el Informe denomina una «cultura de la información».
- Garantizar el acceso equitativo y generalizado a las infraestructuras proporcionadas por las TIC.
- Controlar los riesgos existentes con el objetivo de alcanzar los beneficios esperados de este proceso evolutivo. El Plan recoge en este sentido, la aspiración de alcanzar logros en campos tan diversos como el económico, de servicios (sanitarios y de formación y educación continua) o laborales.

Para el Informe Bangemann los elementos constitutivos en los que se basa la Sociedad de la Información son las redes, los servicios básicos y las aplicaciones. De acuerdo con el último objetivo enunciado de controlar los riesgos inherentes a la Sociedad de la Información, desde la UE se ha ido creando un marco normativo destinado a la regulación de sus diversas manifestaciones. Uno de los ejemplos más significativos de esta normativa es la Directiva 2000/31/CE, que se refiere a la Sociedad de la Información como la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información.

9 MENÉNDEZ MATO, J.C. (2005). *El contrato vía Internet.* Bosch.

4. La Protección de los Datos Personales

Los servicios que incluye la Sociedad de la Información son diversos, y por lo tanto diversas son también las modalidades de tratamientos de datos personales realizados como consecuencia de su desarrollo, a título de ejemplo podemos señalar:

- Servicios de acceso a Internet
- Buscadores
- Servicios de comunicaciones (Chat, correo electrónico, etc.)
- Comercio electrónico
- ...

Las nuevas formas de comunicación y los nuevos medios utilizados para el proceso de la Información han pasado a ocupar un lugar central en los procesos productivos y de generación de riqueza, cambiando radicalmente nuestros hábitos y formas de relacionarnos. Dicha situación implica la aparición de nuevas oportunidades, pero a un tiempo, pueden afectar directamente a principios y derechos que es necesario proteger jurídicamente mediante el establecimiento de límites y obligaciones.

Tal y como establece Davara Rodríguez[10], "*las nuevas tecnologías ya no son solamente una herramienta útil en las funciones rutinarias de gestión y control económico de la empresa en su faceta interior; las nuevas tecnologías tienen su verdadero interés en la unión (casi por naturaleza) con las telecomunicaciones y su apertura hacia el mundo exterior que, al no tener límites aparentes, plantea serias dudas en cuanto al respeto de los derechos básicos de los individuos y su estructuración en una diferente organización social, que permita no poner puertas al campo, con el paralelo respeto a los derechos de la persona y su desarrollo en libertad dentro de la convivencia*".

Los tratamientos de información, suponen una serie de riesgos[11] ciertos para los derechos de las personas:

10 DAVARA RODRÍGUEZ, M. (2006). *Manual de Derecho Informático 8ª Edición*. Thomson Aranzadi. Pág 25.

11 Boletín Oficial de las Cortes Generales (1999). *Informe de la Comisión Especial de Redes Informáticas del Senado. Aprobado por acuerdo del Pleno del Senado en su sesión del día 17 de diciembre de 1999*. Senado, núm. 812, de 27 de diciembre.

- **Dualización entre sociedades:** Existe el riesgo de que se produzca una nueva dualización entre el Primer y el Tercer Mundo y también una dualización en el seno de las llamadas sociedades "avanzadas": entre los que tienen capacidad económica para acceder a la información y los que no la tienen, entre los que saben y los que no saben y, entre estos últimos, entre aquellos que no saben por que no quieren o los que no saben por que no pueden o no disponen de los medios necesarios para ello. En relación con esta idea se ha enunciado el riesgo de la denominada "*brecha digital*". La misma puede darse también en forma de una dualización territorial, entre aquellos que vivan en zonas que por su situación económica, geográfica y poblacional dispongan de la llamada "banda ancha" y los que tengan que conformarse con el arcaico acceso a las redes telefónicas rurales.
- **Metamorfosis del mundo laboral:** El puesto de trabajo tradicional, en el que se entra a la misma hora y se comparte un mismo espacio, tiende a desaparecer. Lo que cuenta es el producto final, no importa desde donde se haga, quién lo haga ni en cuanto tiempo. Las nuevas tecnologías de la información, que pueden significar un gran paso de cara a eliminar tareas rutinarias, corren también el riesgo de convertirse en el origen de la vulneración de derechos de los trabajadores.
- **Aparición de nuevos monopolios:** El mercado no siempre acoge como producto final de consumo ni lo mejor, ni lo más útil, ni lo técnicamente más perfeccionado y ni siquiera lo más barato. No todos los actores implicados en estos mercados se encuentran en igualdad de condiciones de competencia y son cada vez menos los que están en disposición de encarar los retos que el mercado demanda.
- **Involución de los sistemas políticos:** Pueden surgir problemas políticos y de representatividad en los estados democráticos. Las TIC como herramienta para la comunicación de masas, representan además un instrumento de poder extraordinario en manos de quien pueda ejercer su control de forma efectiva.
- **Utilización ilícita de las nuevas tecnologías:** Pueden existir riesgos que puedan poner en peligro derechos subjetivos de las personas, como son los derechos al honor, a la intimidad personal, y al secreto de las telecomunicaciones. En el ámbito de Internet, la determinación de la autoría por los hechos ilícitos producidos, respecto a la elaboración de su contenido y su difusión constituyen problemas de difícil solución. Igualmente la prohibición, la retirada o el secuestro de información considerada como ilícita o ilegal por atentar contra valores y bienes jurídicos de

todo tipo dignos de protección, constituyen una cuestión a tener en cuenta. En el ámbito que nos atañe, los nuevos medios de tratamiento de la información representan un riesgo evidente para la intimidad, el honor, la propia imagen y, en lo que se refiere al objeto de este curso, al derecho a la protección de datos personales.

5. Seguridad jurídica en la Sociedad de la Información

Ante el escenario descrito, resulta evidente que la Informática y en general todos los aspectos que pueden englobarse bajo el término “Sociedad de la Información” presentan una serie de características especiales y poseen la entidad suficientecomo para justificar un desarrollo normativo específico.

La relación entre Informática y Derecho se pone de manifiesto en múltiples aspectos como:

- Uso de nuevas vías para la celebración de contratos.
- Empleo de medios probatorios más seguros y adecuados a las necesidades demandadas por la sociedad.
- La generación (y a su vez, necesidad de protección adecuada) de una nueva modalidad de bienes que ha derivado en la aparición de un nuevo tipo de propiedad industrial sobre los programas de ordenador.

5.1. El Derecho Informático

Puede definirse como la aplicación del conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y las comunicaciones y que tiene por objeto la aplicación de las Tecnologías de la Información al Derecho.

Se trata de un ámbito que, debido sus aspectos regulatorios, se encuentra por un lado, en permanente evolución exigiendo un esfuerzo constante de adecuación a los nuevos riesgos y necesidades y por otro lado es una materia en la que hay que tener siempre muy presente la regulación a nivel internacional y europeo, ya que su objeto es la regulación de actividades que tienen como una de sus principales características, su capacidad para rebasar fronteras.

En España, la base del Derecho Informático es el reconocimiento constitucional del uso de la informática, con las limitaciones que se establezcan legalmente (artículo 18.4 de la

Constitución Europea). A partir de este artículo se han ido aprobando un gran número de normas.

Dichas normas, dictadas en el marco de la Sociedad de la Información, ha propiciado que algunos autores comiencen a hablar del Derecho informático, como una rama autónoma e independiente del ordenamiento. De acuerdo con este planteamiento, quedarían comprendidos dentro del derecho informático, entre otros, los siguientes aspectos:

- Telecomunicaciones
- Protección de Datos.
- Delitos informáticos.
- Responsabilidad civil en materia informática.
- Firma Electrónica.
- Contratación informática y electrónica
- Creación, distribución, explotación y utilización de *hardware* y *software.*
- Protección del honor, la intimidad personal y familiar y la propia imagen.
- Servicios y entorno de la Sociedad de la información.
- Etc.

6. El derecho a la intimidad

6.1 Los orígenes: "The Right of be let alone"

El origen del concepto jurídico de intimidad es anglosajón y en concreto procede del derecho norteamericano.

El primer antecedente es la definición contenida en la obra "*The Elements of Torts*", del Juez Thomas A. Cooley, en la que se recogía la idea en estos términos: «*the right to be let alone*», que podríamos traducir como el derecho a ser dejado en paz).
En 1890 Samuel Warren y Louis Brandeis publican en la Harvard Law Review un artículo titulado «The Right to Privacy». En él se definía el nuevo derecho en los siguientes términos:

«*Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society* […] *Now the right to life has come to mean the right to enjoy life, - the right to be let alone*»[12].

Desde esta idea primaria, la lucha por el reconocimiento de un ámbito de privacidad inherente a toda persona ha sido una constante en la evolución de las sociedades democráticas. Por esta razón, desde los años sesenta y setenta del pasado siglo, la posibilidad de ingerencias en la intimidad de las personas se ha ido incrementando de forma constante y espectacular, planteando a su vez nuevos retos para el Derecho que no puede ser ajeno a una realidad que evoluciona constantemente.

6.2 Evolución histórica

La privacidad, sus distintas acepciones, es un hecho histórico y como tal, es cambiante. Así lo percibimos a lo largo de los siglos. Para comprender la forma en la que los tratamientos

12 *«Los cambios políticos, sociales y económicos entrañan el reconocimiento de nuevos derechos y el derecho común, en su eterna juventud, se amplía para satisfacer nuevas demandas de la sociedad (…), ahora, el derecho a la vida ha evolucionado hasta significar el derecho a disfrutar de la vida, el derecho a ser dejado en paz».*

de información afectan al ámbito que definimos como "*intimidad*", debemos comprender de cómo se originó dicho concepto y cual ha sido su evolución a lo largo del tiempo hasta convertirse en el derecho fundamental que proclama nuestra constitución

Históricamente podemos identificar los antecedentes de reconocimiento de lo que entendemos actualmente por derecho a la intimidad. Así por ejemplo, podemos citar la Real Cédula dictada por Felipe II en 1592 donde, en relación con la correspondencia, se consagraba el derecho al secreto de las comunicaciones de la siguiente forma:

«porque es el instrumento con que las gentes se comunican, y además de ser ofensa de Nuestro Señor abrir las cartas, estas han sido y deben ser inviolables a todas las gentes..., y de necesidad cessaría o se impediría notablemente el trato o comunicación si las dichas cartas y pliegos no aduviessen y se pudiessen embiar libremente y sin impedimento, ..., os mando hagais pregonar ..., que ninguna justicia ni persona ni particular, eclesiástica ni seglar, se atreva a abrir ni detener las dichas cartas, ni a impedir a que ninguno escriva ..., y por ningún caso que sea de manifiesta sospecha de ofensa a Nuestro Señor o peligro de la Tierra, no abrireis ni deterneis vos ni ellos las dichas cartas ni despacho; porque además de que lo contrario me terné deservido, mandaré proveer del remedio que convenga».

No obstante, debemos referirnos, no a este antecedente sino a otros posteriores mucho mejor relacionados con la materia que nos ocupa. En efecto, la primera aparición del término aparece en el contexto de la revolución burguesa y a lo largo del siglo XIX este fue afirmándose en relación con el deseo de establecer un ámbito de la realidad a la intervención del Estado. Como consecuencia de este enfoque encontramos una distinción que nos es familiar, la que separa los ámbitos público y privado.

Se trata por de una distinción relativamente reciente y que se relaciona con el concepto de propiedad, delimitada mediante la declaración de ámbitos excluidos de la intervención del Estado. Así, las primeras acepciones de intimidad se relacionaban con ámbitos de propiedad principalmente en relación al domicilio o al contenido de la correspondencia.

Ya hemos mencionado que el término se utilizó por primera vez en el sentido jurídico que

hoy le otorgamos en 1890, en el artículo de Warren y Brandeis "*The right to the privacy*". que sostiene la intimidad como un derecho autónomo:

«La prensa está excediendo en todas las direcciones los límites más obvios de la corrección y de la decencia. El chismorreo ya no es recurso de los ociosos y depravados sino que se ha convertido en un oficio desempeñado con tanta diligencia como descaro. Para satisfacer el gusto de los más depravados, los detalles de las relaciones sexuales se desparraman a lo ancho de las columnas de la prensa diaria. Para entretener al indolente, columna tras columna se llena de vacuos chismes, que sólo pueden haberse obtenido mediante intrusiones al círculo de la vida doméstica».

En este sentido, los primeros casos que llegaron a los tribunales versaban fundamentalmente sobre el derecho a la propia imagen, considerada como un reflejo del derecho a la intimidad. Así, tres años después de la publicación del citado artículo se produjo una decisión judicial dictada en un caso en el que el demandante, actor y estudiante de Derecho, había visto en un periódico propiedad del demandado un retrato suyo formando parte de un concurso de popularidad, al que él se oponía. La sentencia estimó la demanda y declaró su "derecho a ser dejado en paz"[13]

Años más tarde, Brandeis fue nombrado Juez de la Corte Suprema, que en 1928 emitió una Sentencia que dio lugar a la cuarta enmienda a la Constitución norteamericana:

«No se violará el derecho del pueblo a la seguridad de sus personas, hogares, papeles y efectos contra registros y detenciones arbitrarias a menos que hubiese causa probable, apoyada por juramento o afirmación que designe específicamente el lugar que haya de registrarse y las personas u objetos de los cuales haya de apoderarse».

Partiendo de esta base, durante los siglos XIX y XX se han llevado a cabo la determinación y la defensa de la intimidad y de la confidencialidad. Las Constituciones que han ido aprobándose han ido configurando una estructura cada vez más sólida alrededor de lo que hoy llamamos intimidad. Así, en el derecho español podemos ver una evolución del derecho a la intimidad, a lo largo de nuestras constituciones y que nos pueden aportar un

13 MAESTRE RODRÍGUEZ, J.A. (2003). *La intimidad: El derecho de autodeterminación personal*. En Nuevas Tecnologías de la Información y Derechos Humanos. Cedecs. Págs. 275 a 284.

óptica general de la consolidación de este derecho:

- **Estatuto de Bayona de 1808.** Artículo 126. Inviolabilidad del domicilio: *«La casa de todo habitante en el territorio español y de las Indias es asilo inviolable: no se podrá entrar en ella sino de día y para un objeto especial determinado por la ley, o por una orden que dimane de la autoridad pública».*
- **Constitución de 1812**. Artículo 306. Inviolabilidad del domicilio: *«No podrá ser allanada la casa de ningún español, sino en los casos que determine la ley para el buen orden y seguridad del Estado»*

- **Constitución de 1837**. Artículo 7. Inviolabilidad del domicilio: *«No puede ser detenido, ni preso, ni separado de su domicilio ningún español, ni allanada su casa sino en los casos y en las formas que las leyes prescriben»*
- **Constitución de 1869.** *«Artículo 5. Nadie podrá entrar en el domicilio de un español, o extranjero residente en España, sin su consentimiento, excepto en los casos urgentes de incendio, inundación u otro peligro análogo, o de agresión ilegítima procedente de dentro, o para auxiliar a persona que desde allí pida socorro. Fuera de estos casos, la entrada en el domicilio de un español, o extranjero residente en España, y el registro de sus papeles y efectos, sólo podrán decretarse por el Juez competente y ejecutarse de día. El registro de papeles y efectos tendrá siempre lugar a presencia del interesado o de un individuo de su familia, y, en su defecto, de dos testigos vecinos del mismo pueblo. Sin embargo, cuando un delincuente, hallado in fraganti y perseguido por la Autoridad o sus agentes, se refugiase en su domicilio, podrán éstos penetrar en él, solo para el acto de la aprehensión. Si se refugiare en domicilio ajeno, procederá requerimiento al dueño de éste».*
  «Artículo 7. En ningún caso podrá detenerse ni abrirse por la Autoridad gubernativa la correspondencia confiada al correo, ni tampoco detenerse la telegráfica. Pero en virtud de auto de juez competente podrán detenerse una y otra correspondencia, y también abrirse en presencia del procesado la que se le dirija por correo».

- **Constitución de 1978:** *Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. 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.
Artículo 20. 1. Se reconocen y protegen los derechos:
A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
A la producción y creación literaria, artística, científica y técnica.
A la libertad de cátedra.
A comunicar o recibir libremente información veraz por cualquier medio de difusión. La Ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.
2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.
3. La Ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.
4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las Leyes que lo desarrollan y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.
5. Solo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

Por último, se hace necesario recoger una norma internacional de vital importancia para la materia que nos ocupa, el artículo 12 de la Declaración Universal de Derechos Humanos:

«Nadie será objeto de injerencias, arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataque a su honra o a su reputación»

7. Actualidad de la intimidad

El concepto de intimidad ha evolucionado de una idea basada en la propiedad privada y la inviolabilidad del domicilio, al enunciado de un derecho fundamental, inherente a la persona. Por medio del derecho a la intimidad el ser humano se reconoce una esfera de la interioridad que permanece inaccesible a las personas que nos rodean. Todo individuo necesita contar con ese refugio de intimidad inexpugnable en el que distinguimos simultáneamente una condición de la personalidad individual y también de la personalidad social. Esta idea es clave y en la práctica se traduce en diversas manifestaciones concretas, como los derechos a la inviolabilidad del domicilio, al secreto de las comunicaciones, o a la protección de datos.

En líneas generales, la intimidad ofrece dos facetas o modos de ejercerse:

- **Negativa**: Implica la facultad del hombre para limitar un reducto al margen de los otros.
- **Positiva**: Relativa al derecho a la propia imagen o al honor o al derecho a la protección de datos personales. En virtud de esta protección, cada individuo tiene derecho a controlar la información referente a su esfera más íntima, que gestionan los demás.

La doctrina del Tribunal Constitucional distingue respecto al derecho a la intimidad los siguientes puntos:

- El derecho fundamental a la intimidad reconocido por el artículo 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares.
- El derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar[14], frente a la divulgación del mismo por terceros y una publicidad no deseada.

14 Tribunal Constitucional. Sala Segunda. Sentencia 231/1988, de 2 de diciembre y Sentencia 197/1991, de 17 de octubre.

- El derecho a la intimidad no garantiza una intimidad determinada, sino el derecho a poseerla, disponiendo a este fin de un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público.

De los tres puntos enunciados, se deducen tres manifestaciones del derecho a la intimidad, que apuntamos a continuación:

- **Intimidad personal:** Refleja la necesidad de que la persona disponga de un reducto íntimo en el que no quepan injerencias como presupuesto indispensable de una vida digna. En palabras del Tribunal Constitucional[15]: *«El derecho a la intimidad personal consagrado en el artículo 18.1 aparece configurado como un derecho fundamental, estrictamente vinculado a la propia personalidad y que deriva, sin duda, de la dignidad de la persona humana que el artículo 10.1 reconoce. Entrañando la intimidad personal constitucionalmente garantizada la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de vida humana»*
- **Intimidad familiar:** Se trata de una extensión de este derecho que va más allá de la persona y que debemos interpretar por el ámbito definido tanto por el núcleo familiar constituido por vínculos de consanguinidad o afinidad como por las modernas formas de convivencia reconocidas en la Ley. De nuevo citando a nuestro Tribunal Constitucional: *«Ciertos eventos que puedan ocurrir a padres, cónyuges o hijos tienen normalmente, y dentro de las pautas culturales de nuestra sociedad, tal trascendencia para el individuo, que su indebida publicidad o difusión incide directamente en la propia esfera de su personalidad. Por lo que existe al respecto un derecho -propio, y no ajeno- a la intimidad, constitucionalmente protegido» «El derecho a la intimidad personal y familiar se extiende no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar, aspectos que, por la relación o vínculo existente en ellas, inciden en la*

15 Tribunal Constitucional. Sala Segunda. Sentencia 231/1988, de 2 de diciembre y Sentencia 57/1994 de 28 de febrero.

propia esfera de la personalidad del individuo que los derechos del artículo 18.1 protegen».

- **Intimidad y derecho a la propia imagen:** En otras ocasiones el derecho a la intimidad aparece conectado con el derecho a la propia imagen, considerada como parte de su intimidad. Sin embargo, la jurisprudencia constitucional deslinda claramente ambos derechos como derechos de acuerdo con la definición del artículo 18.1 CE. Como señala Carreras Serra[16], «*las vulneraciones a la intimidad son intromisiones en la vida privada de las personas que revelan aspectos que deben quedar reservados al ámbito de privacidad a que todo el mundo tiene derecho. En cambio, el derecho a la propia imagen es independiente de la lesión a la vida íntima de las personas, y su objetivo es salvaguardar en un ámbito propio y reservado, aunque no íntimo, los rasgos físicos de una persona frente a la acción y el conocimiento de los demás»*. El Tribunal Constitucional ha declarado en este sentido[17]: *«Dado el carácter autónomo de los derechos garantizados en el artículo 18.1 de la Constitución Española, mediante la captación y reproducción de una imagen puede lesionarse al mismo tiempo el derecho a la intimidad y el derecho a la propia imagen, lo que ocurriría en los casos en los que la imagen difundida, además de mostrar los rasgos físicos que permiten la identificación de una persona determinada, revelara aspectos de su vida privada y familiar que se han querido preservar del público conocimiento.*

  En tales supuestos la apreciación de la vulneración del derecho a la imagen no impedirá, en su caso, la apreciación de las eventuales lesiones al derecho a la intimidad que se hayan podido causar, pues, desde la perspectiva constitucional, el desvalor de la acción no es el mismo cuando los hechos realizados sólo pueden considerarse lesivos del derecho a la imagen que cuando, además, a través de la imagen pueda vulnerarse también el derecho a la intimidad».

7.1 Intimidad y privacidad

Existen dos conceptos en ocasiones no bien definidos: Intimidad y Privacidad, que sin

16 CARRERAS SERRA, L. (2003). *Derecho Español de la Información.* UOC. Universitat Oberta de Catalunya.

17 Tribunal Constitucional. Sala Segunda. Sentencia 156/2001, de 2 de julio. Fundamento Jurídico Tercero.

duda conviene aclarar de cara al estudio del derecho a la protección de datos personales. Nos encontramos en presencia de términos cuya acepción no es unánime en nuestra doctrina.

La confusión se debe en parte a la traducción e introducción en el debate del término inglés "privacy". En derecho anglosajón, fundamentalmente en los Estados Unidos de Norteamérica, la tutela de los derechos personales se fundamenta en la "*privacy*", derecho constitucional no expresamente reconocido en la Constitución americana, y cuyo concepto se correspondería con el castellano intimidad, pero entendiendo ésta de manera más amplia que el mero poder de exclusión del conocimiento de los demás de la esfera personal.

Este concepto se ha ido ampliando hasta introducir una nueva acepción de "*privacy*", la "*privacy of autonomy*" o la "*informational privacy*", que engloba el derecho a la protección de datos personales que en derecho anglosajón no es un derecho fundamental de la personalidad, sino que se clasifica como una manifestación más del derecho a la intimidad.

Sea cual sea el motivo de la confusión, hay que tener en cuenta que en nuestro derecho privacidad e intimidad no son términos sinónimos Lo íntimo es la "*zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*". Nos referimos cuando aludimos a esta idea al conjunto de sentimientos, pensamientos e inclinaciones más internos, como la ideología, la religión, sin olvidar a las sectas como postula el Profesor Suñé[18] o creencias, las tendencias personales que afectan a la vida sexual, la salud así como otras inclinaciones que deseamos mantener en secreto.

La *privacidad* es un concepto más amplio, que comprende la intimidad, pero que va más allá: "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*". Se trata de un concepto variable en función de situaciones personales y sociales y que hace referencia, además de a la intimidad, al ámbito de la persona formado por su vida familiar, aficiones, bienes particulares y actividades personales. Todos estos aspectos, además de los íntimos, constituyen una esfera que se debe proteger también de la intromisión.

[18] SUÑÉ LLINÁS, E. (1999). *Tratado de derecho informático. Introducción y protección de datos personales (Volumen I; 2ª edición).* Madrid: Servicio de publicaciones de la facultad de derecho. Universidad Complutense de Madrid. Pág. 150.

8. Fundamentos políticos y sociales de la protección de datos

La Sociedad de la Información, el impacto de las Tecnologías y las Comunicaciones así como el Derecho a la Intimidad configuran el escenario que ha tenido como consecuencia el reconocimiento del derecho a la protección de datos y la progresiva creación de lo que se ha denominado "**cultura de protección de datos",** que consiste en una creciente sensibilización hacia el valor que tienen los datos personales, sensibilización que ha ido de la mano de un mayor conocimiento de los derechos y medios de protección que el ordenamiento jurídico ofrece en este sentido.

Corresponde pues, en este punto, y como medio para completar nuestra exposición, comentar los fundamentos políticos y sociales que sustentan este derecho, partiendo de la ponencia de Spiros Simitis en el transcurso de la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, celebrada en Cracovia del 25 al 26 de abril de 2005[19].

Spiros Simitis señala como única vía para la regulación de la protección de datos, la configuración del mismo como un derecho fundamental, en contraposición a otras opciones y derivadas de las nociones de intimidad y privacidad:

«La innegable relación entre la protección de datos y los derechos fundamentales de las personas, como también recalcaba la Directiva de 1995, predispone a todas las regulaciones relativas al uso de datos personales. Ni la Unión Europea, tal y como demuestra la Constitución, ni los legisladores nacionales, tienen elección. Su primera y más importante tarea es establecer normas vinculantes que deben regir cualquier recopilación y procesamiento de datos personales. En otras palabras, la Constitución rechaza tanto los intentos generalizados de percibir la protección de datos tan solo como una moderna variación de los derechos de la propiedad y que promueven, por tanto, la mercantilización de los datos personales, como las eternas demandas de abandonar interferencias legislativas y sustituirlas en nombre de la flexibilidad y globalización por una autorregulación virtualmente sin límites. Dicho de otro modo: la autorregulación es sin duda un instrumento válido, pero solo siempre que se observe y practique como un medio auxiliar que complemente las decisiones legislativas. Ejemplos como el de las

19 Agencia de Protección de Datos de la Comunidad de Madrid (2008) .Revista Datos Personales en su ejemplar de Enero.

regulaciones elaboradas en el sector de investigación o las normas en los códigos de conducta establecidos por la Directiva de 1995 son precisamente típicos para comprender la autorregulación»

Continua su exposición, dibujando el escenario haciendo referencia al aumento de los tratamientos de datos personales, constante fija en la Sociedad de la Información:

«Independientemente de si cualquier ley ha tenido realmente éxito garantizando un procesamiento exclusivamente determinado por fines inequívocos establecidos de antemano y descritos de forma concluyente a las personas implicadas, la combinación de una tecnología de procesamiento en constante mejora y de políticas preventivas a largo plazo no solo aumenta el número de datos recopilados, sino que al mismo tiempo aumenta en gran medida la presión de un número también creciente de terceros que acceden a los datos. Los bancos de ADN pueden ser un instrumento indispensable de investigación, pero cuando por fines perfectamente legitimados para el proyecto de investigación específico, los datos médicos y genéticos se combinan con una amplia gama de datos sobre el estilo de vida, el interés de las agencias de seguridad y sanitarias es inmediatamente primordial. Además, cualquier empresa que en el contexto de sus propias actividades reúna datos personales, pronto descubre su valor económico y en consecuencia multiplica los esfuerzos por capitalizar este activo nuevo e importante alquilando o vendiendo los datos, según se ha mencionado anteriormente»

«La aparentemente convincente disminución de las consecuencias de procesamiento que realmente ponen en peligro las actividades de las personas con el estado es una asunción indefendible. Las visiones de Orwell podrían haber sido plausibles en los primeros días de la protección de datos, donde el mero coste de establecer grandes bancos de datos parecía ser absolutamente prohibitivo para usuarios privados potenciales. En consencuencia, en un principio muchos países limitaron deliberadamente la legislación al sector público. Pero el enorme progreso de la tecnología pronto mostró lo falso de esta premisa. El ordenador omnipresente es un signo inequívoco de un procesamiento igualmente omnipresente. Además, la experiencia muestra que la intensidad del uso de datos personales en el sector privado no es en modo alguno inferior a las actividades similares del sector público. Las bases de datos de empresas que administran y comercializan datos personales pueden competir con éxito en cualquier momento con las recopilaciones de las

agencias públicas. Así, no nos sorprendamos de que los servicios públicos renuncien cada vez más a elaborar sus propias bases de datos y, en vez de ello, obtengan su acceso permanente a recopilaciones que, como las establecidas por compañías de tarjetas de crédito, seguros, telecomunicaciones y agencias de viajes, proporcionan un gran número de información que necesitan de un modo decididamente más meticuloso y definitivamente más actualizado».

Para finalizar reflexiona sobre los temas que en este momento deben ocupar el centro del desarrollo de la protección de los datos de carácter personal. En primer lugar, el autor identifica una actitud pasiva por parte de muchos ciudadanos ante la recogida y tratamiento de sus datos personales:

«La actitud pasiva, y a veces incluso fatalista, con respecto al siempre creciente procesamiento de datos personales tiene, para empezar, dos orígenes que la mayor parte del tiempo están simplemente reprimidos. En primer lugar, no es nada sorprendente que las empresas privadas hayan abandonado obviamente su posición inicial categóricamente negativa con respecto a las normas limitativas del procesamiento de datos. Y no tanto por la necesidad de aumentar la confianza de los clientes reales y potenciales que últimamente se subraya tan explícitamente, sino porque casi todas las actividades de procesamiento adicionales están cubiertas por cláusulas estandarizadas de consentimiento y, como en el caso de las tarjetas de clientes, por remuneraciones especiales. Es algo natural, y además una experiencia muy conocida en la historia de las relaciones contractuales, que el interés de los clientes se centra primero y principalmente en el coche que él o ella deseen comprar, el trabajo al que él o el.la aspiran, el crédito que él o ella necesitan, el lugar al que él o ella esperan viajar. Y, al igual que en el pasado nadie leía nunca cláusula por cláusula un contrato particular, tampoco nadie presta atención especial a una declaración de consentimiento situada en alguna parte. Además, pequeños obsequios aceleran la firma y devalúan aún más las disposiciones de consentimiento. Internet, y en particular ofertas como aquellas para una mayor seguridad, son más ejemplos de lo preparados que estamos para consentir independientemente de las consecuencias»

Spiros Simitis reclama una mayor conciencia de los efectos que estos tratamientos pueden implicar:

«La cuestión decisiva ya no es, como entre 1970 y 1990, qué datos pueden recopilarse en general y si algunos estarían estrictamente exentos o al menos solo se usarían excepcionalmente. La última y única cuestión pertinente y realista es, de hecho, si y en qué circunstancias el procesamiento de datos personales debe rechazarse categóricamente, incluso cuando técnicamente el acceso fuera posible. (...)

Las sociedades democráticas solo garantizarán su existencia si se preguntan continuamente si las actividades privadas y públicas respetan y garantizan sus principios de gobierno. Ninguna sociedad democrática puede pretender la eternidad. Todas son frágiles y por lo tanto dependen de un autoanálisis crítico constante. Una protección de datos eficaz es una prueba de la capacidad para establecer y conservar estructuras democráticas»

Finaliza Spiros Simitis definiendo el papel y las características que deberán tener las normas de protección de datos como herramienta fundamental en la defensa de estos derechos y principios:

«Si estas expectativas tienen que asumirse en serio, las normas de protección de datos deben concebirse y observarse como partes de una regulación abierta, capaces de reaccionar continuamente a los cambios tecnológicos así como a las modificaciones del uso de datos personales, y por lo tanto esforzándose continuamente por la mejor protección posible. Esta es la razón por la que el legislador noruego ya limitó hace unos años la aplicación de la ley de protección de datos a un período de tiempo claramente definido, e impuso así tanto al parlamento como al gobierno un discurso incesante sobre la necesidad de nuevos enfoques, un ejemplo seguido por algunos otros países. La protección de datos nunca debería verse como una regulación estática, sino siempre como un proceso dinámico que no tiene fin»

II. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Introducción

En la actualidad es posible acceder a casi todos los aspectos de la vida de las personas y, lo que es más importante, reconstruirla a partir de datos aparentemente inofensivos o carentes de interés pudiéndose tomar decisiones basadas en los mismos.

Todo ello pone en manos del número creciente de personas, organizaciones y Estados, con acceso a los medios necesarios, un poder de control sobre los titulares de los datos que afecta directamente a su libertad, identidad y dignidad.

En España, si bien la formulación del derecho a la protección de datos tiene su soporte en la Constitución Española de 1978, ha sido la jurisprudencia del Tribunal Constitucional la que ha dado carta de naturaleza al mismo.

Esta calificación tiene una gran importancia, ya que implica el reconocimiento de que estamos ante una exigencia esencial de la sociedad y la puesta a disposición de los titulares de los datos del mayor nivel de protección que el ordenamiento jurídico puede ofrecer así como de los instrumentos de tutela más poderosos.

Conviene por tanto, iniciar un camino en el que se repasarán las principales características de los derechos fundamentales y los derechos de la personalidad para, en un análisis posterior centraremos en el derecho a la protección de datos

2. Los derechos fundamentales

2.1. Aproximación a los derechos fundamentales de la personalidad

Los derechos fundamentales son aquellos derechos humanos reconocidos y asegurados por el ordenamiento jurídico positivo e interno de cada Estado, en la mayoría de los supuestos en su texto constitucional, y que habitualmente gozan de una protección o tutela reforzada.

Encontramos en esta definición la referencia al término derechos humanos, que en ocasiones se utiliza como sinónimo de derecho fundamental, pero que en esencia alude a aquellos derechos que concretan los valores inherentes a la dignidad de la persona y que, por ello, lejos de nacer de una concesión de la sociedad política, han de ser reconocidos y garantizados por ésta.

Castán[20] se refiere a ellos como "*aquellos derechos fundamentales de la persona humana -considerada tanto en su aspecto individual como comunitario- que corresponde a ésta por razón de su propia naturaleza (de esencia, a un mismo tiempo, corpórea, espiritual y social) y que deben ser reconocidos y respetados por todo Poder o autoridad y toda norma jurídica positiva, cediendo, no obstante, en su ejercicio, ante las exigencias del bien común*".

En este sentido, las **libertades públicas** son aquella parte de los derechos fundamentales que representan ámbitos de actuación individual en los cuales el Estado no puede intervenir; es decir, vienen referidas a los derechos tradicionales de signo individual y tienen como finalidad prioritaria el garantizar las esferas de autonomía subjetiva. Son facultades y ámbitos de acción autónoma de los individuos o grupos salvaguardadas frente a la intervención estatal.

En lo relativo a la expresión *"derechos de la personalidad"* nos referimos con ella a un conjunto de derechos, generalmente fundamentales, inherentes a cada individuo, por constituir una manifestación de la dignidad de la persona y estar orientados a garantizar su

20 CASTÁN TOBEÑAS, J. (1979). *Los derechos del hombre*. Prólogo de Luis Legaz Lacambra. Reus. Madrid. Pag 13

propia esfera individual.

Se trata de una expresión que procede del derecho civil, donde se ha utilizado para designar a un conjunto heterogéneo de derechos subjetivos (vida e integridad, honor, intimidad e imagen, nombre, etc….) que se caracterizan negativamente por su naturaleza no patrimonial, y positivamente por proteger determinados atributos de la personalidad.

En efecto, el ordenamiento jurídico concede una serie de derechos a las personas, imponiéndole también otros tantos deberes y, consiguientemente, un ámbito de responsabilidad que denominamos "*esfera jurídica de la persona*", la cual se subdivide, a su vez, en una esfera personal (la que aquí nos interesa) y una esfera patrimonial.

Dentro de la primera, se reconoce a la persona una parcela de poder jurídico, orientada a la conservación y desenvolvimiento de su individualidad, a la protección de bienes de distinta naturaleza (personales, familiares y sociales) y cuya salvaguarda es imprescindible para la dignidad humana.

A lo largo de la Historia, y hasta el nacimiento del Estado moderno, el conocimiento que las Administraciones han tenido de sus ciudadanos ha sido muy escaso y habitualmente limitado a temas muy específicos como aspectos tributarios o de prestación de determinados servicios. Y si en los ámbitos mencionados no existían intrusiones significativas, menos aún podían darse intromisiones en la esfera privada.

Por contra, a lo largo de los siglos XIX y XX estos llamados "*derechos de la personalidad*" se fueron haciendo necesarios y, constatada en la práctica la limitada efectividad de las sanciones penales en este campo, fueron desarrollándose afirmando la protección del Derecho privado a la persona en la totalidad de sus manifestaciones y atribuciones.

Los derechos de la personalidad son derechos concebidos desde dos aspectos:

- Se constituyen en primer lugar como límites a la actuación del derecho público.
- Sirven como vías para permitir a los tribunales la reparación del daño moral causado por la violación injusta de estos derechos

Debemos detener un instante nuestro análisis para comentar las características principales de los derechos de la personalidad:

- **Derechos esenciales**. Son derechos asociados de forma indisoluble a la naturaleza humana y como tales cumplen una función esencial en relación con el principio de igualdad jurídica.
- **Derechos absolutos o de exclusión**. Los derechos de la personalidad suponen un poder inmediato y directo sobre el aspecto de la personalidad de que se trate, siendo oponibles frente a todos -*erga omnes*-.
- **Derechos inherentes.** Son derechos personalísimos, habiendo sido identificado su objeto con los bienes más superiores de la persona. Los detenta todo individuo desde que nace hasta que fallece, sin excepción, como derechos innatos u originarios.
- **Derechos extrapatrimoniales o personales.** Como **c**onsecuencia de las características enunciadas anteriormente, se deriva su indisponibilidad e intransmisibilidad, irrenunciabilidad, imprescriptibilidad y la no susceptibilidad de acción subrogativa o indirecta . No obstante, el hecho de ser calificados como derechos extramatrimoniales no implica que en caso de vulneración puedan derivarse consecuencias patrimoniales mediante la vía del resarcimiento del daño, dirigida a garantizar una compensación equivalente a aquellos bienes personales que hayan sido vulnerados.

2.2. Naturaleza jurídica de los derechos fundamentales

Los derechos fundamentales comparten una serie de características en común:

- **Son Imprescriptibles.** No están afectados por la prescripción, sin que, por tanto, se adquieran ni pierdan por el simple transcurso del tiempo.
- **Son Inalienables.** No transferibles a otro titular, lo que sí es posible, en términos generales, en los demás derechos subjetivos.
- **Son Irrenunciables.** El sujeto de los mismos no puede renunciar a su titularidad, no puede desprenderse de ellos, a diferencia de lo que sucede por lo general en los

derechos no fundamentales.

- **Son Universales.** Deben ser reconocidos a todos los hombres.

En el pasado se atribuyó también a los derechos fundamentales el carácter de absolutos, queriendo afirmar con ello que podían ejercitarse de modo ilimitado; esta cualidad les fue atribuida, por ejemplo, en la Declaración de Derechos del Hombre y del Ciudadano, proclamada por la Revolución francesa en 1789.

No obstante, resulta necesario establecer cierto límites, aceptando que el ejercicio de los derechos fundamentales debe someterse a criterios como el orden público, el bien común y, por supuesto, los derechos de los demás.

Podemos distinguir tres clases de **límites** a los derechos fundamentales:

- Límites contenidos en el texto constitucional.
- Límites recogidos en las leyes de desarrollo de los derechos fundamentales.
- Límites establecidos por normas supranacionales.

El ejercicio de los derechos fundamentales puede colisionar con otros bienes también protegidos por la Constitución. Las disposiciones constitucionales relativas a los derechos fundamentales no suelen prever todos los hipotéticos conflictos de esta índole que puedan ocurrir en la práctica. Por ello, los límites establecidos a los derechos fundamentales no pueden agotarse en las menciones explícitas que se realizan en las distintas disposiciones constitucionales.

Como regla general, la garantía de los derechos fundamentales de terceras personas será el fundamento principal para justificar este tipo de medida, y en todo caso, la actividad restrictiva del ejercicio de los derechos reconocidos en el texto constitucional deberá derivar de un conflicto *objetivamente perceptible* del derecho fundamental con otros bienes, valores, principios o derechos constitucionales.

Por lo tanto, cabe aplicar a los derechos fundamentales otros límites, más allá de los impuestos por el propio texto constitucional.

En este sentido, el artículo 53.1 de la Constitución Española señala:

«Los derechos y libertades reconocidos en el Capítulo II del presente Título vinculan a todos los poderes públicos. Sólo por Ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades que se tutelarán de acuerdo con lo previsto en el artículo 161.1.a)»

La presente reserva de ley puede considerarse como de carácter genérico, ya que afecta a todos los derechos reconocidos en el Capítulo segundo del Título primero de la Constitución, se concreta y se refuerza con respecto a aquellos derechos fundamentales reconocidos en la sección 1.ª del Capítulo segundo de este mismo título a través de la reserva de Ley Orgánica prevista en el artículo 81 del texto constitucional:

«1. Son Leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.

2. La aprobación, modificación o derogación de las Leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto.»

Por último, debemos hacer referencia a que los derechos fundamentales y libertades públicas deben aplicarse también conforme a los tratados internacionales sobre Derechos Humanos, teniendo en cuenta, tal y como postula el Profesor Carretero Sánchez[21] que un Tratado es un *Acto Internacional creador de un determinado efecto jurídico, la formación de normas convencionales obligatorias entre los Estados-partes.*

En este sentido el artículo 10.2 CE dispone:

«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

[21] CARRETERO SÁNCHEZ, S. (2005). *Nueva introducción a la Teoría del Derecho.* Madrid: Dykinson. Pág. 79

por España.»

Merece la pena ahora exponer los criterios que se establecen para la resolución de conflictos en la materia que nos atañe. En este sentido, los límites que como hemos visto pueden establecerse a los derechos fundamentales en ningún caso pueden constituirse en restricciones de carácter absoluto.

Esto supone que, en caso de colisión entre el ejercicio del derecho fundamental en cuestión y el bien que se constituya en su límite, no debe siempre, de forma automática, ceder el primero, sino que previamente deberá haber una labor de ponderación de los bienes en conflicto[22].

Este examen lo llevan a cabo los órganos jurisdiccionales que conozcan de los diferentes conflictos que puedan darse en la práctica; la labor de estos órganos será armonizar las relaciones entre las libertades y derechos, así como los valores, bienes o principios integrados en nuestro ordenamiento jurídico de cara a encontrar un equilibrio entre los mismos. Los órganos jurisdiccionales deberán tener en consideración las especificidades de cada supuesto práctico para ofrecer una respuesta particular al mismo.

La jurisprudencia nos ofrece una serie de elementos a tomar en cuenta para realizar correctamente la labor de ponderación de los bienes jurídicos en caso de conflicto: así, la sentencia del Tribunal Constitucional 154/2002[23], de 18 de julio, en su fundamento jurídico octavo, afirma, resumiendo la doctrina expuesta a lo largo de los años por este tribunal, que todo acto o resolución que límite derechos fundamentales ha de cumplir con los siguientes requisitos:

- Asegurar que las medidas limitadoras son necesarias para conseguir el fin perseguido.
- Tener en cuenta el denominado principio de proporcionalidad, que exige que el

22 Entre otras ver las Sentencias del Tribunal Constitucional 81/1983, de 10 de octubre (Fundamento jurídico tercero), 104/1986, de 17 de julio (Fundamento jurídico sexto), 105/1990, 5 de junio (Fundamento jurídico segundo), 123/1993, 19 de abril (Fundamento jurídico sexto), 286/1993, de 4 de octubre (Fundamento jurídico quinto), 288/1994, de 27 de octubre (Fundamento jurídico primero), 127/2000, de 16 de mayo (Fundamento jurídico tercero), 112/2000, de 5 de mayo (Fundamento jurídico quinto) y 154/2002, 18 de julio (Fundamento jurídico octavo).

23 Tribunal Constitucional. Pleno. Sentencia 154/2002, de 18 de julio.

sacrificio del derecho individual cuyo ejercicio pueda ser limitado se encuentre en una relación equilibrada con la finalidad perseguida por la actividad restrictiva.

- Respetar el contenido esencial del derecho constitucional limitado, lo que supone, que la restricción no puede hacer impracticable el derecho o dificultar su ejercicio más allá de lo razonable. En este sentido, la jurisprudencia constitucional ha defendido siempre la fuerza expansiva de los derechos fundamentales, lo que conlleva que los órganos jurisdiccionales deberán siempre interpretar sus límites de forma restrictiva. Además, en el caso de que el bien jurídico que opera como límite sea otro derecho fundamental, deberá buscarse la realización simultánea de ambos derechos en grado más óptimo.

2.2.1 Clasificación de derechos fundamentales

Son varias las clasificaciones que de los derechos fundamentales pueden hacerse, según los distintos criterios o puntos de vista que se tengan en cuenta si bien, en este punto, se opta por señalar tres tipos, que corresponden con los respectivos momentos del proceso histórico de su aparición: los derechos civiles, los políticos y los sociales.

A. Derechos civiles

Los **derechos civiles** son aquellos que afectan de modo más directo a la persona en cuanto que se refieren a los aspectos más íntimos de ésta; se cuentan entre ellos, como más importantes, el derecho a la vida y a la integridad física, el derecho a la propiedad, a la libertad, a la dignidad, a la libertad de pensamiento y de conciencia, a la libre profesión de una religión, a la inviolabilidad del domicilio, por citar algunos ejemplos.

Teniendo en cuenta la naturaleza de estos derechos, es explicable que fueran los primeros respecto de los cuales se exigió su reconocimiento, por lo que no sorprende su mención en las primeras Declaraciones; así, en la Declaración de derechos del buen pueblo de Virginia (1776), precedente inmediato de la Declaración de independencia de los Estados Unidos, se dice que "l*os hombres... tienen ciertos derechos innatos..., a saber: el goce de la vida y de la libertad, con los medios de adquirir y poseer la propiedad y de buscar y obtener la felicidad y la seguridad*", y en la Declaración francesa que encabeza la Constitución de

1791, se enumeran como "*derechos naturales e imprescriptibles... la igualdad, la libertad, la seguridad y la propiedad*".

B. Derechos políticos

Logrado el reconocimiento de los derechos civiles, las aspiraciones se dirigen hacia los **derechos políticos**, que son los que garantizan de modo general la intervención del ciudadano en la vida pública. Entre ellos incluimos el derecho al sufragio, a participar en el gobierno, a exigir del poder que rinda cuentas de su actividad, al control de los impuestos o a la libertad de asociación y reunión.

La regulación de estos derechos y libertades se produce por vía constitucional a lo largo del siglo XIX, siglo que se caracteriza (debido al influjo, sobre todo, de la ideología liberal) por una constante preocupación por el perfeccionamiento de las instituciones democráticas y por establecer el juego de garantías requerido para conseguir un equilibrio entre el poder y los ciudadanos.

C. Derechos sociales

Por último, quedaba por desarrollar el principio de la igualdad, proclamado en las Declaraciones y en los textos constitucionales, pero que no había pasado de esa consagración puramente formal y, por tanto, teórica.

Durante el siglo XIX, y especialmente en su segunda mitad, coincidiendo con los movimientos sociales basados en la conciencia de clase se presentan estas reivindicaciones dirigidas al reconocimiento de los **derechos sociales** del hombre en cuanto miembro de una sociedad. Son derechos en materias como la salud, la educación o la vivienda.

2.2.2. Protección de los derechos fundamentales

La calificación de un derecho como derecho fundamental tiene una relevancia práctica

importante ya que ofrece al titular del mismo una serie de instrumentos de protección cualificada que permitan garantizar el bien jurídico protegido en cada caso, si bien los sistemas de garantías varían en cada país.

La competencia para la protección y tutela de estos derechos está unas veces atribuida a los Tribunales ordinarios y otras a un órgano jurisdiccional específico, al que los ciudadanos pueden acudir ejercitando el recurso de amparo y que también tienen capacidad para conocer en recursos de inconstitucionalidad contra leyes y disposiciones normativas con fuerza de ley. Existe también una protección de rango internacional: el Tribunal Europeo de derechos del hombre, ante el que pueden comparecer los ciudadanos en queja frente al propio Estado cuando entiendan que éste ha vulnerado sus derechos fundamentales[24].

Ciñéndonos al caso español, nuestro ordenamiento jurídico destaca entre los diversos modelos de protección de los derechos fundamentales que podemos encontrar en los países de nuestro entorno, por el alto nivel amparo que otorga a los mismos.

La Constitución Española recoge en el Capítulo IV de su Título Primero (artículos 53 y 54) los siguientes instrumentos para garantizar los derechos fundamentales:

«***Artículo 53.***

1. Los derechos y libertades reconocidos en el Capítulo II del presente Título vinculan a todos los poderes públicos. Sólo por Ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades que se tutelarán de acuerdo con lo previsto en el artículo 161.1.a.

2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo II ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.

24 Este Tribunal sólo actúa respecto a los Estados que suscribieron el Convenio de Roma de 1950, que creó aquél, y entre los que se cuenta España

3. El reconocimiento, el respeto y la protección de los principios reconocidos en el Capítulo III, informará la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las Leyes que los desarrollen.

Artículo 54.

Una Ley orgánica regulará la institución del Defensor del Pueblo, como alto comisionado de las Cortes Generales, designado por éstas para la defensa de los derechos comprendidos en este Título, a cuyo efecto podrá supervisar la actividad de la Administración, dando cuenta a las Cortes Generales.»

Como podemos observar, el artículo 53 diseña las grandes líneas del sistema de protección de los derechos fundamentales en el ordenamiento español, mientras que el artículo 54 instituye la figura del Defensor del Pueblo como órgano de supervisión de la Administración pública y de tutela no jurisdiccional de los ciudadanos frente a la misma.[25]

Como regla general se entiende que los derechos fundamentales presentan siempre dos facetas: derechos subjetivos y valores objetivos:

- En cuanto **derechos subjetivos**, los derechos fundamentales otorgan facultades o pretensiones que las personas pueden hacer valer en relaciones concretas frente a otros sujetos, normalmente públicos.
- En cuanto **valores objetivos**, los derechos fundamentales encarnan bienes jurídicos que el ordenamiento debe proteger y promocionar, con independencia de las concretas situaciones en que puedan hallarse los particulares: toda norma o acto público debe respetar, esos valores siendo inválida en otro caso. Dichos valores constituyen, además, un criterio privilegiado de interpretación del entero ordenamiento jurídico.

25 No obstante, hay que tener en cuenta en relación con los citados artículos, que estos no agotan el régimen de protección previsto para los derechos fundamentales. No todas las garantías de los derechos fundamentales están aquí recogidas.

Esta identificación, que ha sido admitida por la jurisprudencia constitucional (entre otras, por las sentencias del Tribunal Constitucional de 14 de julio de 1981, 11 de abril de 1985 y 12 de abril de 1988), es de particular relevancia para el sistema de garantías: mientras que el funcionamiento de los derechos fundamentales como valores objetivos sólo requiere la existencia de alguna forma de control judicial de validez de las normas, su condición de derechos subjetivos exige, además, cauces procesales abiertos a la invocación de aquéllos por los particulares.

Como expresamente exige el artículo 53.1 CE, los derechos fundamentales vinculan a todos los poderes públicos, cualquiera que sea su ámbito (estatal, autonómico y local) o carácter (legislativo, ejecutivo, judicial). En este punto han de ser incluidas, por lo tanto, las garantías de los derechos fundamentales frente al legislador y el sistema de protección frente a las actuaciones de las Administraciones públicas y del Poder Judicial.

En cuanto a la actividad del legislador, los derechos fundamentales suponen un límite que podemos verificar en el procedimiento agravado de reforma constitucional para cualquier revisión de la Constitución Española que afecte a la Sección 1.ª del Capítulo II del Título I (artículo 168 de la Constitución). Además, se establece una reserva de ley sobre cualquier regulación tendente a desarrollar o, simplemente, a incidir sobre los derechos fundamentales.

En lo que se refiere a la protección de los derechos fundamentales frente a las actuaciones de las Administraciones públicas y del Poder Judicial, hay que destacar que estas constituyen el más poderoso instrumento en manos de los particulares, pues les permiten accionar ante un juzgado o tribunal y defender sus derechos en un proceso.

Los derechos fundamentales son derechos de rango constitucional; pero conviene subrayar que, a diferencia de lo que ocurre en materia de declaración de inconstitucionalidad de las leyes, la protección jurisdiccional de los derechos fundamentales frente a las Administraciones públicas y el Poder Judicial no es monopolio del Tribunal Constitucional. Esta corresponde primariamente a los tribunales ordinarios mientras que el Tribunal Constitucional cumple sólo una función subsidiaria o de garantía última.

Por último, en cuanto al Defensor del Pueblo, regulado el el artículo 54 de la Constitución,

se trata de una institución no judicial que, entre otras funciones, canaliza las quejas de los ciudadanos, entre ellas las que puedan referirse a la materia de los derechos fundamentales. La Constitución, legitima al Defensor del Pueblo para interponer recursos de inconstitucionalidad y de amparo. Hay que tener en cuenta, además la tipificación en el Código Penal del delito de obstaculización en los procesos de investigación del Defensor del Pueblo, por parte de autoridades o funcionarios.

3. Origen del derecho fundamental a la protección de datos de carácter personal

Ya hemos apuntado que el enunciado y la protección de los derechos fundamentales han sufrido una continua evolución a lo largo de las diferentes etapas históricas. No siempre se han reconocido los mismos derechos fundamentales, ni se ha concedido siempre el mismo nivel de protección. Por tanto, los derechos fundamentales no deben considerarse como categorías estancas y cerradas, sino que debe asumirse que su reconocimiento jurídico responde al interés, diferente en cada momento histórico y en cada cultura, de dar solución a necesidades cambiantes, en relación a las diversas amenazas y riesgos.

Este es el caso del Derecho a la Protección de Datos de Carácter Personal, nacido de las nuevas demandas individuales derivadas de los riesgos de la informatización de todos los aspectos de la vida, que hace necesarios nuevos instrumentos de protección.

Se hace relevante en este punto realizar una breve revisión teminológica puesto que en general, las sentencias dedicadas, por nuestro Tribunal Constitucional, en relación a este tema, hablan de un derecho fundamental a la protección de datos de carácter personal, pero en otras usan la expresión “libertad informática” o “derecho a la autodeterminación informativa”. Si bien las tres se utilizan en referencia al mismo derecho, cada una de ellas subraya una dimensión distinta de esta figura.

La primera se centra sobre todo, en los medios o técnicas de los que se vale el derecho, para la protección del bien jurídico en riesgo, aunque también puede entenderse que alude al fin que persigue. La segunda, “libertad informática”, refleja el fondo último al que responde y el contexto en el que se sitúa. Por último “Derecho a la autodeterminación

informativa", apunta a su esencia. Expresa el contenido material del derecho y quizás aporta mayor precisión sobre su significado.

En todo caso, hay que tener presente que, pese a que se ha generalizado la formulación "derecho a la protección de datos de carácter personal", y es la que utilizaremos aquí en la gran mayoría de las ocasiones, podemos encontrar las otras dos denominaciones. De hecho la fórmula "autodeterminación informativa" fue la utilizada por el Tribunal Constitucional Federal de Alemania en su Sentencia de 1983, en la que enjuiciaba la adecuación a la Ley Fundamental de Bonn de la Ley del Censo, por lo que puede afirmarse que se encuentra en el origen del reconocimiento de este derecho.

3.1. Antecedentes

3.1.1. La sentencia del Tribunal Constitucional Federal de Alemania

El primer antecedente directo de la formulación del mismo, es la Sentencia dictada en 1983 por el Tribunal Constitucional Federal Alemán que constituye el primer paso para la construcción y elaboración del derecho reconociendo y acuñando como decimos la expresión "*derecho a la autodeterminación informativa*". En la breve exposición que se lleva a cabo para marcar las directrices de la sentencia, el Tribunal alemán argumenta:

«(...) en las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1º, de la Ley Fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona»

Continúa la Sentencia:

«(...) las limitaciones de este derecho a la "autodeterminación informativa" sólo son admisibles en el marco de un interés general superior y necesitan un fundamento legal

basado en la Constitución, que debe corresponder al imperativo de claridad normativa inherente al Estado de Derecho»

Se reconocía así por primera vez y de forma específica, el derecho del individuo a disponer sobre los tratamientos realizados con sus datos personales. En relación a esta sentencia, en primer lugar, hay que reconocer el acierto de los recurrentes al plantear la amenaza que encierra el tratamiento automatizado de datos. Para ellos, la protección de la información más íntima de la persona no fue lo relevante, sino que se centraron en la solicitud de reconocimiento de la importancia de aquellos datos que, sometidos a un tratamiento que los relacione con otra información relativa al individuo, puede revelar los más variados aspectos de su vida y comportamiento. Los recurrentes centraron su atención por lo tanto, no en la protección estricta del dato personal, que por sí solo puede resultar intrascendente, sino en la limitación del tratamiento informatizado de cualquier dato de carácter personal, que conduce al fenómeno que ellos denominan "enmallamiento". Este es un elemento fundamental al no limitar su planteamiento a solicitar la tutela y protección a los datos denominados *sensibles*, sino también para aquellos que sin pertenecer a la esfera más próxima al individuo, son susceptibles de dañar su imagen o el ejercicio pleno de sus derechos.

3.1.2. Fundamento constitucional

El primer fundamento del derecho a la protección de datos se encuentra en el texto constitucional. Nuestra constitución de 1978, dispone en su artículo 18:

«Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales,

telegráficas y telefónicas, salvo resolución judicial.

4. 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 artículo 18.1 de la Constitución «garantiza el honor, la intimidad personal y familiar y la propia imagen», otorgando categoría de derechos fundamentales lo que habilita la tutela prevista por el artículo 53.2:

«2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo II ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.»

Se trata de un régimen de protección que no tiene precedente en nuestro derecho constitucional y que otorga un reconocimiento en la protección de la personalidad que se completa con la cláusula general del artículo 10.1 de la Constitución:

«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.»

Este reconocimiento constitucional de la dignidad humana y el libre desarrollo de la personalidad resulta muy importante, pues no sólo se encuentra en la base del reconocimiento de otros derechos, sino que además cumple la función de principio interpretativo de nuestro ordenamiento jurídico[26].

Centrándonos en el artículo 18.4 de la Constitución, básico para el reconocimiento posterior del derecho fundamental a la protección de datos, es de destacar en primer lugar como la previsión de la limitación legal del uso de la informática se incluye en un precepto dedicado a la protección de la intimidad en general. De esta redacción han derivado las

26 Tribunal Constitucional. Sala Primera. Sentencia 214/1991, de 11 de noviembre.

distintas interpretaciones posteriores que, hasta las sentencias del Tribunal Constitucional que veremos a continuación, centraron el debate sobre si el artículo 18.4 de la Constitución recoge un derecho derivado de la intimidad, o si por el contrario constituye un derecho autónomo e independiente.

La redacción que hoy conocemos está influida por la Constitución portuguesa de 1976 cuyo artículo 35 dispone:

«1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrá exigir la rectificación de los datos, así como su actualización.

2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos»

En este sentido el Borrador y el Anteproyecto constitucional español, tenían el siguiente contenido:

«La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos»

Este texto fue debatido en la Comisión Constitucional del Congreso en la que se dieron dos posturas enfrentadas. Por un lado se planteaba innecesaria la limitación al considerar que la garantía del honor y la intimidad estaba contemplada en el apartado tercero del artículo 18 de la Constitución de una manera general[27]. Por el contrario, Gastón Sanz, del Grupo Mixto, planteó la necesidad de su inclusión de forma que la aplicación de los límites en el uso de la informática se extendiera a todos los derechos fundamentales en lugar de restringirse al derecho al honor y a la intimidad. Finalmente se encontró una vía intermedia entre ambas posturas[28] basada en la idea de que el verdadero riesgo aparece cuando estos tratamientos de información inciden en el ejercicio de los derechos. Por esta razón se

27 Defendida por D. Sancho Rof, en nombre de Unión de Centro Democrático
28 Defendida por D. Miquel Roca i Junyent

incluyó la segunda parte del artículo 18.4 CE que insiste en que los límites de la informática garanticen el pleno ejercicio de los derechos de los ciudadanos.[29]

De esta forma, se llegó a la redacción actual que, en vez de dedicar un artículo completo de la Constitución a los tratamientos informáticos, los incluye entre los derechos mencionados, dando lugar al denominado derecho a la autodeterminación informativa. La Constitución rechazaba así la configuración de un derecho a la protección de datos y lo vinculaba al derecho al honor y a la intimidad dándole una formulación negativa al limitar el uso de la informática, en vez de una positiva que hubiera sido más adecuada permitiendo prever explícitamente el ejercicio de derechos como el acceso y control de los tratamientos de datos por el interesado.

3.1.3. Antecedentes directos en España

En España, y en el mismo año en el que se pronunciaba el Tribunal alemán en la sentencia expuesta con anterioridad, nuestro Tribunal Constitucional adoptaba también una importante resolución sobre este tema.

Se trata de la **Sentencia del Tribunal Costitucional 110/1984, de 26 de noviembre**[30] dictada con motivo del recurso de amparo número 575/1983, relativo a la vulneración del derecho a la intimidad por la exigencia de aportar certificaciones de las operaciones de determinadas cuentas bancarias. En dicha sentencia el Tribunal Constitucional vino a reconocer que era preciso ampliar las fronteras en cuanto a la protección de los derechos del individuo se refiere, debido a que el concepto de vida privada o de "calidad de vida" no había permanecido inalterable, sino más bien se podía afirmar que el ser humano adquiere nuevas pretensiones respecto a su esfera de intimidad.

Algunos de los puntos más importantes de la argumentación del Tribunal Constitucional son los siguientes:

«3. Prescindiendo ya de esos temas tangenciales ha de examinarse lo que constituye la argumentación básica del recurrente, que consiste, como se ha dicho en que la exigencia

29 Enmienda número 117 propuesta por Roca en nombre de Minoría Catalana
30 Tribunal Constitucional. Sala Primera. Sentencia 110/1984, de 26 de noviembre.

de aportar las certificaciones relativas a las operaciones activas y pasivas de las cuentas abiertas en determinados establecimientos de crédito constituye una vulneración del derecho a la intimidad personal y familiar reconocido en el art. 18.1 CE.

El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. Pero su idea originaria, que es el respeto a la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad de domicilio y de la correspondencia que son algunas de esas libertades tradicionales tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y del desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad. (...)

4. Hecha esa indicación previa, procede examinar la cuestión concreta planteada por el recurrente que, en realidad, se desdobla en dos: una, en qué medida el conocimiento de las cuentas bancarias por la Administración a efectos fiscales debe entenderse comprendido en la zona de la intimidad constitucionalmente protegida, y otra cuestión, consistente en determinar en qué medida y aunque aquel conocimiento no esté protegido por el derecho a la intimidad se puede a través de la investigación fiscal conocer hechos pertenecientes a la esfera de la estricta vida personal y familiar.

5. Respecto a la primera cuestión la respuesta ha de ser negativa, pues aún admitiendo como hipótesis que el movimiento de las cuentas bancarias esté cubierto por el derecho a la intimidad nos encontraríamos que ante el fisco operaría un límite justificado de ese derecho. Conviene recordar, en efecto, que como ya ha declarado este TC, no existen derechos ilimitados. Todo derecho tiene sus límites que en relación a los derechos fundamentales establece la Constitución por sí misma en algunas ocasiones, mientras en

otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales sino también otros bienes constitucionales protegidos (TC S 8 Abr., FJ 7, Sentencia, 29 Ene., FJ 5.ª). Ahora bien, el conocimiento de las cuentas corrientes puede ser necesario para proteger el bien constitucionalmente protegido que es la distribución equitativa del sostenimiento de los gastos públicos, pues para una verificación de los ingresos del contribuyente y de su situación patrimonial puede no ser suficiente en ocasiones la exhibición de los saldos medios anuales y de los saldos a 31 Dic. (...)

(...) Ahora bien, estos datos en sí no tienen relevancia para la intimidad personal y familiar del contribuyente como no la tiene la declaración sobre la renta o sobre el patrimonio. El recurrente parece insistir especialmente en la gravedad de que la investigación, de las cuentas comprenda las operaciones pasivas, pues a nadie le importa en qué gasta cada cual su dinero. Pero el conocimiento de una cuenta corriente no puede darse si no se contempla en su integridad. Las operaciones pasivas pueden ser también reveladoras de una anómala conducta fiscal, como ocurría, entre otros supuestos que podrían citarse con la retirada de una masa importante de dinero sin que se explique el destino de la misma, que ha podido trasladarse de una situación de transparencia fiscal a otra menos o nada transparente.

6. En realidad, el recurrente insiste más bien en la segunda cuestión: la posibilidad de que a través de la investigación de las cuentas se penetre en la zona más estricta de la vida privada, ya que en nuestra sociedad, una cuenta corriente puede constituir "la biografía personal en números" del contribuyente, como en frase gráfica dice el mismo recurrente.

(...) desde este punto de vista el recurso no se plantea tanto frente a una presunta vulneración actual del derecho a la intimidad como en previsión de vulneraciones futuras y eventuales. Pero el recurso de amparo no tiene carácter cautelar y este Tribunal no puede pronunciarse sobre lesiones de un derecho fundamental que aún no se ha producido. Sin embargo, y dada la índole de las alegaciones que hace el recurrente sobre el contenido de la Ley de Reforma Fiscal y el derecho a la intimidad, no resulta superfluo formular algunas observaciones sobre esta cuestión.

(...) Es cierto que la Ley de Reforma Fiscal permite investigar los saldos y movimientos de

las cuentas así como los documentos y demás antecedentes relativos a los mismos (art. 45 Ley de Reforma Fiscal) y la OM 14 Ene. 1978 dice que en los casos que se proceda a la investigación "podrá la Inspección exigir al obligado a colaborar la aportación de todos los datos, antecedentes y circunstancias que, referentes al sujeto investigado, existan en cualquiera de sus oficinas en el plazo total máximo de 15 días desde que así se le pidiere" (Regla 5 C de la citada OM). Pero no es exacto afirmar que la Ley y la OM citadas otorgan unas facultades ilimitadas a la Inspección. La Ley prevé para la investigación de las Cuentas Bancarias un conjunto de requisitos como son: a) la autorización ha de proceder de ciertos órganos que se enumeran taxativamente (Ley de Reforma Fiscal art. 42.1); b) en la autorización deben precisarse una serie de extremos, tales como las cuentas y operaciones que han de ser investigados, los sujetos pasivos interesados, la fecha en que la actuación debe practicarse y el alcance de la investigación (ibídem); c) la investigación se llevará a cabo según procedimientos específicos y, en su caso, con citación del interesado y en presencia del Director de la entidad bancaria de que se trate (Ley de Reforma Fiscal art. 42.2); d) los datos o informaciones sólo podrán utilizarse a los fines tributarios y de denuncia de hechos que pueden ser constitutivos de delitos monetarios o de cualesquiera otros delitos públicos; e) se recuerda con especial energía el deber de sigilo que pesa sobre todas las autoridades y funcionarios que tengan conocimiento de los datos revelados en la investigación. (...)»

El Tribunal Constitucional terminaba desestimando el recurso, aportando un enfoque al problema limitado a la privacidad y entendiendo que el mismo tiene unos límites que han de respetarse.

Otras sentencias importantes en la evolución jurisprudencial seguida hasta el reconocimiento llevado a cabo por las STC 290 y 292 de 2000, fueron relativas a:

- **Aplicación del artículo 18.4 de la Constitución (STC 254/1993[31])**: Dictada en resolución al caso de un ciudadano al que el Gobierno Civil de Guipúzcoa le denegó acceso a los datos que de él poseía. Se trata de la primera vez que se alegó el artículo 18.4 de la Constitución y el Tribunal Constitucional señaló al respecto: *«Derecho a la libertad frente a las potenciales agresiones a la*

31 Tribunal Constitucional. Sala Primera. Sentencia 254/1993, de 20 de julio.

dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos». La sentencia añade que no es posible aceptar que *«el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados (...) son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos»*

- **Tratamiento del Número de identificación Fiscal (NIF), respecto a la normativa de protección de datos (STC 143/1994)[32]*:*** Esta sentencia admitió la constitucionalidad del Número de Identificación Fiscal, tal como está regulado en la actualidad[33]. Se trata de una sentencia basada también en la concepción de la protección de datos como una manifestación del derecho a la intimidad.
- **Utilización de datos personales para propósitos diferentes de los que fueron recabados:** Sobre este asunto versan todas las sentencias dictadas en los años 1998 y 1999. Todas ellas enlazan con la doctrina enunciada en las sentencias anteriores al analizar el uso de datos contenidos en un fichero de afiliación sindical para la confección de una lista de trabajadores que habían secundado una huelga. Analizaremos, en particular, las Sentencias del Tribunal Constitucional 11/98[34] y 94/98[35], ya que las demás se remiten a ellas en su fundamentación. Las sentencias subrayan la importancia que tiene en los tratamientos de datos personales, la finalidad para la que se recogieron dichos datos. Así, junto con el consentimiento libre e informado del afectado o la autorización legal, la finalidad se convierte en factor determinante de la protección de datos limitándose el uso que de ellos pueda hacerse, y prohibiendo que se aprovechen para otros objetivos diferentes, no comprendidos en el consentimiento del titular de los datos personales o en la habilitación legal: *«una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita y,*

32 Tribunal Constitucional. Sala Primera. Sentencia 143/1994, de 9 de mayo.

33 Código necesario en las relaciones de los contribuyentes con la Administración tributaria, y en todas aquellas relaciones de carácter patrimonial entre particulares. Real Decreto 338/1990, de 9 de marzo, modificado por el Real Decreto 1393 /1998, de 4 de agosto.

34 Tribunal Constitucional. Sala Primera. Sentencia 11/1998, de 13 de enero

35 Tribunal Constitucional. Sala Segunda. Sentencia 94/1998, de 4 de mayo.

en consecuencia, prohíbe tajantemente el sudo de los datos para finalidades distintas de las que motivaron su recogida (...)». Pero más allá de estas consideraciones, la importancia de las sentencias radica en que en ellas, el Tribunal Constitucional ya apunta a la idea de hallarnos un nuevo derecho fundamental que se materializa en el derecho a controlar el flujo de datos que conciernen a una persona. Este derecho integraría, entre otros, la posibilidad del ciudadano a oponerse al tratamiento de los datos personales y la imposibilidad de que estos datos se destinen a fines distintos a los que motivaron su recogida: *«(...) no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la "privacidad" según el neologismo que reza en la Exposición de Motivos de la LORTAD-, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Tratan de evitar que la informatización de los datos personales propicie comportamientos discriminatorios».* Se iba abandonando así la visión tradicional de la protección de datos como manifestación del derecho a la intimidad.

3.2 Sentencias del Tribunal Constitucional en el año 2000

La **Sentencia 290/2000**[36]**,** se dictó en relación con las impugnaciones contra la LORTAD promovidas por el Parlamento y por el Consejo Ejecutivo de la Generalidad de Cataluña en lo relativo a la competencia sobre los ficheros de titularidad privada radicados en su territorio, desestimándolas. En ella, el Tribunal Constitucional considera que no se ha producido una invasión o lesión de las competencias autonómicas, sino que, por el contrario, la atribución a la Agencia de Protección de Datos estatal de las facultades relativas a esos ficheros resulta ser una consecuencia de la aplicación de lo previsto en el artículo 149.1.a) de la Constitución y, en general, de la naturaleza propia de los derechos fundamentales.

Debido al transcurso del tiempo desde la interposición del recurso hasta la fecha de

36 Tribunal Constitucional. Pleno. Sentencia 290/2000, de 30 de noviembre.

sentencia, algunos de los artículos impugnados ya habían sido modificados por la LOPD, de forma que el Tribunal Constitucional únicamente se pronunció sobre determinados artículos de la LORTAD, en concreto el 21, 24 y 40.

Por su parte, en la **Sentencia 292/2000**[37], el Tribunal entró en las cuestiones de fondo, pero ya sobre el texto de la entonces recién aprobada LOPD. Interpretó aquellos puntos de la Ley que afectan a las restricciones que, en el marco de los ficheros y tratamientos de las Administraciones Públicas, el legislador impuso a las facultades que integran el derecho a la autodeterminación informativa. Su aspecto más relevante es aquel que da carta de naturaleza en nuestro ordenamiento jurídico a un nuevo derecho fundamental: el derecho fundamental a la protección de datos. El Tribunal Constitucional se pronuncia en este sentido, de acuerdo con la Carta de los Derechos Fundamentales de la Unión Europea, aprobada en Niza, por la cumbre de Jefes de Estado y de Gobierno de la Unión Europea. La **Carta de los Derechos Fundamentales de la Unión Europea** de forma lacónica, y sin ninguna referencia a la intimidad o la privacidad, dispone en su **artículo 8:**

«Toda persona tiene Derecho a la protección de los datos de carácter personal que le conciernan».

«El respeto de estas normas quedará sujeto al control de una autoridad independiente»

La sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, dictada en resolución del recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo, es la que definitivamente ha reconocido que el Derecho fundamental a la protección de datos personales deriva directamente de la Constitución y debe considerarse como un Derecho autónomo e independiente. Se trata de un texto básico en la materia y por esta razón, es necesario resaltar sus puntos más importantes:

«4. Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no solo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido

37 Tribunal Constitucional. Pleno. Sentencia 292/2000, de 30 de noviembre.

trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.

Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando 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 que es también, «en sí mismo, un derecho o libertad fundamental» (STC 254/1993), de 20 Jul., FJ 6). Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el Anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no solo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.

(...) el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo «un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»», lo que se ha dado en llamar «libertad informática» (FJ 6, reiterado luego en las SSTC 143/1994 FJ 7, 11/1998 FJ 4, 94/1998 FJ 6, 202/1999 FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre

los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998 FJ 5, 94/1998.

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE , con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran. (...)

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 Jul., FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 Jul., FJ 5; 144/1999, FJ 8; 98/2000, de 10 Abr., FJ 5; 115/2000, de 10 May., FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué

datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 Oct., FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona.

(...)

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer

uso de lo así conocido (SSTC 73/1982, FJ 5; 110/1984 FJ 3; 89/1987 FJ 3; 231/1988 FJ 3; 197/1991 FJ 3, y en general las SSTC 134/1999 , 144/1999 y 115/2000), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).»

4. Configuración actual del derecho a la protección de datos

En relación al **contenido,** el fundamento jurídico séptimo de la Sentencia 292/2000, termina ofreciendo una definición al respecto:

«De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos 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 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. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.»

El Tribunal Constitucional propone una clasificación para determinar el contenido del

derecho:

- Poderes de disposición.
- Derecho a conocer la identidad de la persona que dispone de los datos.
- Derecho a conocer la finalidad del tratamiento.

En todo caso, la pregunta que cabe hacerse ante la formulación de un nuevo derecho es ¿para qué sirve?, es decir ¿cuál es el bien jurídico protegido y que facultades otorga?

En este sentido Pablo Lucas Murillo de la Cueva[38] establece:

«Este derecho sirve para poner en manos de cada uno de nosotros los instrumentos para definir qué aspectos de nuestra vida deseamos -o no nos importa en determinadas ocasiones- que manejen otros. Es decir, para controlar el acceso a nuestros datos personales, a las informaciones de cualquier tipo que nos identifiquen directa o indirectamente, y su uso por terceros, ya sean estos sujetos públicos o privados.

El control que nos ofrece este derecho fundamental descansa en dos elementos principales. El primero es el del consentimiento del afectado como condición de licitud de las actividades de captación y utilización de datos personales por terceros. Consentimiento libre e informado que permite a la persona a la que se refieren autodeterminarse informativamente. No obstante es claro, que en ciertas ocasiones ha de ser posible tratar información personal sin que medie la autorización del afectado. Por eso, y aquí viene el segundo elemento, la ley puede autorizarlo expresamente, bien de forma general al darse las circunstancias por ella previstas o caso por caso. Así, el consentimiento y habilitación legal son los títulos que justifican el tratamiento de datos personales.

Ahora bien, que, por mediar cualquiera de ellos, sea lícito recogerlos y utilizarlos no significa que el afectado pierda su capacidad de autodeterminación en este ámbito. Al contrario, dispone de una serie de facultades -de derechos- que completan su poder de disposición y de control, empezando por el de revocar la autorización cuando la hubiere

38 LUCAS MURILLO P. (2005). *Texto de la conferencia que tuvo lugar el 24 de octubre de 2005 en la sede de la Agencia Catalana de Protección de Datos* [En línea]. Disponible en :www.apd.cat [2011, 10 de enero]

prestado. Facultades que tienen por objeto ejercer su poder de consentir el tratamiento de sus datos con pleno conocimiento de las consecuencias de su decisión y, luego, reaccionar contra quienes hagan un uso indebido de ellos.

Así, integran el contenido activo de este derecho los siguientes elementos:

1) Ser informado en la recogida de datos
2) Conocer la existencia de ficheros y tratamientos de datos personales
3) Acceder a ellos para comprobar qué información personal del afectado contienen
4) Obtener la rectificación de los que no sean exactos
5) Obtener la cancelación de los que no deban ser tratados o hayan perdido la calidad que en su día justificó el tratamiento
6) Oponerse a un tratamiento cuando no se requiera, conforme a la ley, el consentimiento del afectado y concurran motivos fundados y legítimos relativos a su concreta situación personal
7) No sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente
8) Ser resarcido de los sufridos a causa de tratamientos que no se ajusten a las condiciones legalmente establecidas
9) Cabe añadir a todo lo anterior ser protegido por las instituciones especializadas creadas ex profeso para defender este derecho fundamental.»

Además de lo dicho anteriormente, en la XXVII Conferencia Internacional de Autoridades de Protección de Datos celebrada en Montreux, Suiza, en los días 13 a 15 de septiembre de 2005 se aprobó una Declaración Final sobre "*La protección de los datos personales y la privacidad en un mundo globalizado*", en la que se mencionan los siguientes principios del derecho a la protección de datos:

- Principio de recogida y proceso legítimo de los datos
- Principio de calidad
- Principio de finalidad y limitación
- Principio de proporcionalidad
- Principio de transparencia,
- Principio de participación individual y en particular, garantía de derecho de acceso

de los interesados

- Principio de no discriminación
- Principio de seguridad de los datos
- Principio de responsabilidad
- Principio de supervisión independiente y sanción legal
- Principio de nivel adecuado de protección en caso de movimientos transfronterizos de datos personales

Por otro lado, la Carta Europea de Derechos Humanos, siguiendo la tónica de textos anteriores, enuncia otro de los principios que ya son inherentes a la protección de datos: el principio que podría denominarse de control independiente. En efecto, al disponer que «*El respeto de estas normas quedará sujeto al control de una autoridad independiente*» está exigiendo la existencia de tal autoridad como requisito para considerar que el derecho a la protección de datos está suficientemente garantizado.

4.1 Naturaleza jurídica del derecho a la protección de datos

La principal consecuencia de la clasificación por el Tribunal Constitucional del derecho a la protección de datos como un derecho fundamental de la personalidad, es su diferenciación definitiva del derecho a la intimidad. Por otra parte, dicha consideración facilita en gran medida el reforzamiento de las garantías, en tanto que permite la aplicación de las garantías constitucionalmente reconocidas a los derechos fundamentales, y que en otro caso, no resultarían accesibles a los afectados.

Nos referimos, por supuesto, al recurso de amparo ante el Tribunal Constitucional, la intervención del Defensor del Pueblo o la garantía de respeto al contenido esencial, instrumentos que desde el propio texto constitucional intentan asegurar el respeto a los derechos fundamentales y libertades públicas que en nuestro ordenamiento alcanzan la consideración de fundamento y valor superior del orden jurídico y la paz social.

Como sumatorio a lo ya anteriormente expuesto, añadiremos que la clasificación efectuada del derecho a la protección de datos tiene como consecuencia la consideración del mismo como:

- **Derecho fundamental independiente, no instrumental.** No estamos ante un derecho que tenga un carácter instrumental frente a otros, como la libertad individual, el honor o la intimidad si bien, en última instancia, la totalidad de derechos fundamentales pueden considerarse instrumentales respecto de la dignidad humana.
- **Derecho innato al hombre.** Se trata de un *derecho innato* del hombre que protege de la revelación y tratamiento no consentido de datos que afecten directamente a aspectos de su personalidad y por tanto, es indiferente el nivel de sensibilidad de dichos datos. En efecto, el riesgo que justifica la protección de este derecho no se reduce al tratamiento de los datos más íntimos o próximos a la esfera personal del titular, sino que va más allá. Protege a la persona frente a los tratamientos no autorizados de cualquier clase de dato personal ya que todos los tratamientos y la información obtenida a partir de ellos, puede ser relevante a estos efectos.
- **Derecho subjetivo privado.** El derecho a la protección de datos de carácter personal tutela el control del titular de los datos frente a injerencias ajenas. El afectado tiene derecho a conocer de qué información disponen los terceros, con qué finalidad se halla registrada en ficheros informáticos y cuál será su utilización, pero al objeto de prohibir cualquier práctica ilícita. Ello no significa que se reconozca al afectado un derecho de propiedad sobre su información, lo que implicaría la calificación de este derecho como patrimonial. El objeto de protección lo constituye la persona y más correctamente el respeto a sus derechos y al libre ejercicio de los mismos.
- **Derecho de exclusión.** Entendido como derecho oponible "*erga omnes*". Se salvaguarda la esfera privada frente a cualquiera, incluso frente a la Administración; ahora bien, ello no significa que se esté ante un derecho absoluto y, sin limitación alguna.

III. MARCO JURÍDICO

1. Introducción

La protección de datos es una materia de creación relativamente reciente. Solo desde 1967, coincidiendo con el desarrollo de la informática, cabe hablar de la existencia de una preocupación del legislador en estos temas, en relación con la protección de la intimidad de las personas.

Para aproximarnos al marco jurídico, seguiremos la clasificación enunciada por D. Agustín Puente Escobar siguiendo la propuesta de Téllez Aguilera[39].

1.1. Orígenes de la protección de datos

El origen de la protección de datos es europeo. Hemos visto ya que la primera formulación del mismo proviene del reconocimiento y la profundización en el derecho a la intimidad personal y familiar, que desde mediados del siglo XX fue incorporándose a los textos constitucionales del continente. Como primer antecedente normativo, citaremos el artículo 12 de la Declaración Universal de los Derechos del Hombre, declaración adoptada en París por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948:

«Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, no de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques»

En el mismo sentido encontramos recogidos este derecho en otras declaraciones del mismo periodo, como el Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales, firmado en Roma el 14 de noviembre de 1950 (artículo 8) o el Pacto de los

39 PIÑAR MAÑAS, J.L. (2006). *Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal*. En Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch/Agencia Española de Protección de Datos/Red Iberoamericana de Protección de Datos.

Derechos Civiles y Políticos, hecho en Nueva York, el 19 de diciembre de 1966 (artículos 17 y 19).

Con estos antecedentes, en 1967 el Consejo de Europa constituyó la Comisión para el Estudio de las Tecnologías de la Información y su potencial incidencias en los derechos de las personas. El resultado de dicha Comisión se recogió en la Resolución 509 de la Asamblea del Consejo de Europa sobre los derechos humanos y los nuevos logros científicos y técnicos que puede ser considerada como el primer origen de lo que después se ha denominado derecho a la protección de datos de carácter personal.

1.2. Primeros desarrollos legislativos

Este primer interés por la protección de los datos personales ante los tratamientos informatizados, impulsó los trabajos que habían dado como resultado la Resolución citada. En septiembre de 1973 el Comité de Ministros del Consejo de Europa, recomendó a los Gobiernos de sus Estados miembros, respecto a la creación de bancos de datos en el sector privado, tener en cuenta determinados aspectos referentes a abusos o mal empleo de la información. Un año después, en septiembre de 1974, realizó una recomendación similar respecto a la creación de bancos de datos en el sector público[40]2. Fruto de esta mayor concienciación fueron apareciendo en estos años los primeros desarrollos legislativos llevados a cabo por los Estados miembros.

El primero de ellos, fue la Ley adoptada en Alemania, en el Land de Hesse, de 7 de octubre de 1970, que es la primera Ley específicamente dedicada a la protección de los datos personales, en este caso, en sus tratamientos por los organismos públicos. En cuando a leyes de ámbito nacional, la primera fue la Ley Sueca de 11 de mayo de 1973. Se trata de una norma cuyo ámbito abarca ya la totalidad de los tratamientos, tanto los llevados a cabo por el sector público como por el sector privado, y crea una autoridad nacional para la protección de datos personales. En EEUU, por su parte, el primer antecedente también data

40 Resoluciones (73) 22, de 26 de septiembre, adoptada durante la 224 reunión de los Delegados de los Ministros, relativa a "la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado", y (74) 29, de 20 de septiembre, adoptada durante la 236 reunión de los Delegados de los Ministros, respecto a "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público".

de esos años. Se trata de la "*Privacy Act*", referida también exclusivamente a los tratamientos llevados a cabo por los organismos públicos.

1.3. Nuevos desarrollos en la protección de datos

Hacemos referencia en este epígrafe, a las normas desarrolladas en el periodo 1975 – 1980. De estas fechas datan las normas de la República Federal de Alemania, Francia, Dinamarca, Austria y Luxemburgo. El 8 de mayo de 1979, el Parlamento Europeo aprobó una Resolución sobre tutela de derechos del individuo frente al desarrollo de la informática. También en este periodo, el derecho a la protección de datos comienza a recogerse explícitamente en los textos constitucionales.

1.4. Normas de tercera generación

A partir de 1980 podemos hablar ya de un etapa marcada por la aprobación de dos textos esenciales:

- Recomendación de la OCDE sobre la circulación internacional de datos personales para la protección de la intimidad, de septiembre de 1980.
- Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, firmado en Estrasburgo el 28 de enero de 1981.

Ambas implican, en palabras de Téllez Aguilera, la aparición de una serie de normas que configuran "*un catálogo, nítidamente diseñado, de derechos de los ciudadanos para hacer efectiva la protección de sus datos personales así como, posteriormente, la irrupción de las exigencias de las medidas de seguridad por parte de los responsables de ficheros*".

Además, de este periodo datan las elaboraciones jurisprudenciales que configuran el derecho a la protección de datos como un derecho fundamental. En estos años, se promulga también el grueso de normas nacionales de protección de datos, tanto en España, como en los países de nuestro entorno.:

Por último, desde los años 90, se han ido aprobando diferentes normas de ámbito internacional. Algunas de ellas tienen en cuenta los aspectos referentes a la protección de datos personales, incluyendo las recomendaciones del Convenio 108 del Consejo de Europa:

- Convenios de Schengen de 19 de enero de 1990.
- Convenio Europol (de 26 de julio de 1995).
- Convenio de Cooperación en Materia Aduanera y creación de un sistema de creación del Sistema de Información Aduanero (de 23 de enero de 1998).

Otras normas fundamentales en este ámbito que se aprobaron durante este periodo son:

- Resolución de 14 de enero de 1990 de la Asamblea General de las Naciones Unidas, relativa a los principios rectores para la reglamentación de los ficheros computerizados de datos personales.
- Directiva 95/46/CE

1.5. Homogeneización de las Leyes de Protección de Datos y nuevos desarrollos

La aprobación de la Directiva 95/46/CE ha implicado que la realización de transferencias internacionales de datos personales con destino a Estados no miembros de la UE, queden limitadas a que dichos Estados garanticen un mismo nivel de protección, lo que en la práctica ha derivado en que las normativas de aplicación de todos los países implicados hayan ido uniformizándose. Por otra parte, el papel de las distintas Autoridades Nacionales de Control, y en concreto la creación del Grupo creado por el artículo 29 de la Directiva, ha derivado en la creación de una misma base normativa. Además, en los últimos años se han ido aprobando también una serie de normas con incidencia en la materia como son:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica.

- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información y en particular del comercio electrónico en el mercado interior.

2. Instrumentos internacionales de protección de datos

2.1 Las directrices de la OCDE

La OCDE es la Organización para la Cooperación y el Desarrollo Económico (OCDE)[41], una organización de cooperación internacional, compuesta por 30 Estados, cuyo objetivo es coordinar sus políticas económicas y sociales. La organización fue fundada en 1961 y tiene como antecedente directo la Organización Europea para la Cooperación Económica.

Sus principales objetivos son:

- Promover el empleo, el crecimiento económico y la mejora de los niveles de vida en los países miembros, y asimismo mantener su estabilidad.
- Ayudar a la expansión económica en el proceso de desarrollo tanto de los países miembros como en los ajenos a la Organización.
- Ampliar el comercio mundial multilateral, sin criterios discriminatorios, de acuerdo con los compromisos internacionales.

El principal requisito para ser país miembro de la OCDE es la obligación de liberalizar progresivamente los movimientos de capitales y de servicios. Los países miembros se comprometen a aplicar los principios de liberalización, no discriminación, trato nacional y trato equivalente.

En lo que se refiere a la protección de datos personales, ante la inmediata introducción de normativa referente a la regulación de la intimidad en aproximadamente la mitad de los países miembros de la OCDE (Austria, Canadá, Dinamarca, Francia, Alemania,

41 En la actualidad, la OCDE es uno de los foros mundiales más influyentes, en el que se analizan y se establecen orientaciones sobre temas de relevancia internacional como economía, educación y medioambiente.

Luxemburgo, Noruega, Suecia y los Estados Unidos habían aprobado ya legislación; Bélgica, Islandia, Países Bajos, España), y con el objeto de impedir vulneraciones de derechos humanos fundamentales, derivados de almacenamiento ilícito de datos personales, exactos o inexactos, abuso o la revelación no autorizada de los mismos, etcétera, la OCDE resolvió dictar una serie de Directrices, que fueron aprobadas mediante una Recomendación que entró en vigor el 23 de septiembre de 1980.

Este interés en la protección del derecho a la protección de datos y la percepción del peligro de que las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de los datos personales con los graves trastornos que ello podría ocasionar en importantes sectores de la economía, como la banca y los seguros, fueron las principales motivaciones para la elaboración de las Directrices. La importancia de las mismas se basa en que representan un consenso sobre principios básicos a asumir por los Estados con la intención de que pudieran incorporarse a las legislaciones nacionales ya existentes o servir de fundamento para la legislación en aquellos países que todavía no dispusieran de ella. Las Directrices fueron elaboradas por un grupo de expertos gubernamentales. Fueron acompañadas de un "Memorándum Explicativo", con la finalidad de proporcionar información acerca del debate que se llevó a cabo y de los razonamientos que subyacen en su planteamiento. En el mismo se destaca como, entre los países miembros de la OCDE, más de un tercio habían promulgado a la fecha una o varias leyes para proteger a las personas frente al uso abusivo de los datos que a ellos se refieren y darles el derecho de acceso a los mismos con vistas a comprobar su exactitud e idoneidad.

Se hacía también referencia a la distinta denominación que estas leyes adoptaban en diferentes países. Mientras en la Europa continental en la práctica común se hablaba de "legislación sobre datos" o de "legislación de protección de datos" *("lois sur la protection des dones"),* en los países de habla inglesa se la conocía generalmente por "legislación de protección de la intimidad".

La OCDE destacaba como los planteamientos adoptados hasta el momento por los diversos países sobre la protección de la intimidad y de las libertades individuales, tenían muchas particularidades en común. Se identificaban una serie de intereses básicos recogidos por todos estos Estados entre los que se citan:

- Necesidad de fijar límites a la recogida de datos personales de acuerdo con los objetivos de quien los recoge y criterios análogos.
- Obligación de restringir el uso de datos para ajustarse a finalidades especificadas abiertamente.
- Crear servicios para que las personas se enteren de la existencia y contenido de los datos y hacer que se corrijan.
- Identificar a las partes responsables del cumplimiento de las pertinentes normas y decisiones de protección de la intimidad.

En líneas generales, todas las leyes analizadas en el momento intentaban cubrir las fases sucesivas del ciclo que comienza con la recogida inicial de datos y que finaliza con la supresión u otra medida análoga. Del mismo modo, se identificaban los planteamientos dispares como la definición del ámbito de la legislación, el acento puesto en diferentes elementos de protección, la implantación detallada de los principios y los mecanismos para la ejecución forzosa. Las normas variaban, por ejemplo, a la hora de entender necesaria la creación de órganos supervisores especiales, la clasificación de los mismos.

En este contexto, las Directrices vinieron a establecer una serie de principios básicos comunes divididos en principios de aplicación nacional e internacional. La importancia de estos principios se demuestra en el hecho de que el documento número 12 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, considera que el cumplimiento de los mismos por parte de los Estados viene a constituir el mínimo necesario para que los mismos puedan ser considerados como oferentes de un nivel adecuado de protección de datos. Se trata, por otra parte, del primer texto que establece de una forma sistemática los principios fundamentales del derecho a la protección de los datos de carácter personal.

2.1.1. Principios básicos de aplicación nacional

Son los siguientes:

- **Principio de limitación de la recogida.** Deberán existir límites en la recogida de datos personales. Los datos se recabarán por medios lícitos y justos y, en su caso,

con el conocimiento o consentimiento del sujeto de los datos.

- **Principio de calidad de los datos.** Los datos personales deberán ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, serán exactos y completos, y mantenerse al día.
- **Principio de especificación de la finalidad.** Los efectos para los cuales se recojan los datos personales deberán especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedará limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.
- **Principio de limitación de uso.** Los datos personales no se revelarán, no se harán disponibles ni se utilizarán de modo diferente a lo especificado salvo que se realice con el consentimiento del sujeto de los datos, o por imperativo legal.
- **Principio de salvaguardas de seguridad.** Los datos personales deberán protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.
- **Principio de apertura.** Se creará una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberán existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos.
- **Principio de participación individual.** Las personas físicas, tienen derecho a:
  - recabar, del controlador de los datos o de otro modo, confirmación e si el controlador tiene o no tiene datos correspondientes a la misma;
  - hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible;
  - que se le den los motivos para ello, en virtud de los subapartados a) y b), si su solicitud fuere denegada y ella pueda impugnar tal denegación, e
  - impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.
- **Principio de responsabilidad.** El controlador de datos deberá ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba.

2.1.2. Principios básicos de aplicación internacional

Son los siguientes:

- Los países miembros deberían tomar en consideración las consecuencias implícitas para los demás países miembros del tratamiento nacional de los datos personales y de su reexportación.
- Los países miembro deberán adoptar todas las medidas razonables y oportunas para garantizar la circulación transfronteriza, ininterrumpida y segura, de los datos personales, incluso el tránsito a través de algún país miembro.
- La circulación transfronteriza de datos personales entre dos países miembros no deberá restringirse, salvo en el caso de que el segundo país aún no haya observado sustancialmente estas Directrices o cuando la reexportación de tales datos soslayase su legislación nacional sobre la intimidad. A su vez, cualquier país miembro podrá imponer restricciones respecto a ciertas categorías de datos personales para las cuales su legislación nacional sobre la intimidad incluya normativas específicas en vista de la índole de tales datos y para las cuales otro país miembro no proporcione protección equivalente.
- Los países miembros deberán evitar la elaboración de leyes, políticas y prácticas en aras de la protección de la intimidad y de las libertades individuales, que creen obstáculos a la circulación transfronteriza de datos personales que superarían las necesidades de tal protección.

En lo relativo a la implantación de estos principios, se limita a las siguientes recomendaciones:

«Al implantar nacionalmente los principios expuestos en las Partes II y III, los países miembros deberían establecer procedimientos o instituciones jurídicas, administrativas u otras para la protección de la intimidad y de las libertades individuales respecto a los datos personales. Los países miembros deberían, en particular, procurar:

a) Adoptar la legislación adecuada.
b) Fomentar y apoyar la autorregulación, ya sea en forma de códigos de conducta o de otro modo.

c) Prever medios razonables para que las personas ejerciten sus derechos.
d) Prever las saciones y recursos suficientes en caso de incumplimiento de las medidas con las cuales se implanten los principios expuestos en las Partes II y III, y
e) Asegurar que no haya discriminación injusta contra los sujetos de los datos»

Estas Directrices se completaron con la adopción, el 22 de noviembre de 1992 de la Recomendación de la OCDE relativa a la Seguridad de los Sistemas de Información, siguiendo la recomendación ya contenida en el documento de 1980 (C(80)58/Final).

2.2. Las directrices de las Naciones Unidas

Las resoluciones de las Naciones Unidas se caracterizan por ser expresiones formales de la opinión o de la voluntad de los órganos de las Naciones Unidas. En materia de protección de datos de carácter personal cobra especial importancia la Resolución 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990[42].

La citada Resolución contiene una lista de los principios mínimos, en materia de protección de datos de carácter personal, que deberán ser adoptados por las legislaciones internas de todos sus Estados miembros:

- Principio de legalidad y lealtad.
- Principio de exactitud.
- Principio de especificación de la finalidad.
- Principio de acceso de la persona interesada.
- Principio de no discriminación.
- Facultad para hacer excepciones.
- Principio de seguridad.
- Supervisión y sanciones.
- Flujo transfronterizo de datos.
- Capo de aplicación.

42 Asamblea General de las Naciones Unidas (1990). Resolución 45/95, de 14 de diciembre de 1990, relativa a los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales

La Recomendación pese a ser breve recoge los principios básicos de protección de datos, así como una serie de directrices que las organizaciones internacionales deberán tener en cuenta a la hora de llevar a cabo tratamientos de datos de carácter personal.

Por tanto y, como hemos tenido oportunidad de analizar, la regulación de la protección de datos de carácter personal a nivel internacional, se limita a la enunciación de principios, que si bien son de obligado cumplimiento para los estados miembros de las organizaciones referidas, no implican un gran nivel de detalle ni garantizan la necesaria coherencia, más allá de las líneas de actuación que implican los mencionados principios.

3. La normativa europea

Las principales referencias, en cuanto a la normativa de nivel europeo, son las siguientes:

- El Convenio 108 del Consejo de Europa
- 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
- Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas
- Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE

3.1. Antecedentes

Como primer antecedente podemos citar las Resoluciones 73/22 y 74/29 del Comité de

Ministros del Consejo de Europa. La Resolución 73/22[43], del Comité de Ministros del Consejo de Europa en materia jurídica, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado (adoptada por el Comité de Ministros el 26 de septiembre de 1973, durante la 224ª reunión de los Delegados de los Ministros) recomienda a los Estados miembros que actúen en defensa de los derechos de las personas ante la utilización de los bancos electrónicos en el sector privado. Por su parte, la Resolución 74/29[44], (adoptada por el Comité de Ministros el 20 de septiembre de 1.974, durante la 236ª reunión de los Delegados de los Ministros), hace lo propio respecto a los ficheros públicos.

Los principios que se reconocían en ambas Resoluciones siguen teniendo vigencia y plena actualidad hoy en día. En cierto modo podemos decir que sus aspectos esenciales se recogen en la normativa actual y, se pueden resumir en los siguientes puntos:

- La información debe ser exacta, mantenida al día, apropiada para el fin con el que fue almacenada y obtenida legalmente.
- El derecho a conocer la información que se tiene almacenada sobre uno mismo es un derecho de todo ciudadano.
- Todas las personas que operan sobre las bases de datos tienen que mantener el secreto y su conducta debe prevenir el mal uso sobre los mismos.
- La seguridad se debe extremar al máximo, con el fin de impedir el acceso a las bases de datos a las personas no autorizadas o evitar el desvío de información hacia sitios no previstos.
- Si la información se utiliza con fines estadísticos, se hará de tal forma que no sea posible relacionarla con la persona en particular.

3.2. El Convenio 108 del Consejo de Europa

El Convenio 108[45] del Consejo de Europa, adoptado en Estrasburgo el día 28 de enero de

43 Consejo de Europa. Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

44 Consejo de Europa. Recomendación R (74) 29. Relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.

45 Consejo de Europa. Convenio 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

1981, supone un hito fundamental en la regulación del derecho a la protección de datos de carácter personal, máxime si tenemos en cuenta que es el primer instrumento internacional de carácter vinculante adoptado en la materia. El Convenio 108 especifica de forma clara los principios y obligaciones de los responsables de tratamientos y de los propios estados signatarios en la protección de la intimidad y la privacidad de las personas en relación con el tratamiento de sus datos. En su exposición de motivos podemos leer:

«Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras.

Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos»

3.2.1. Contenido

El Convenio recoge los principios contenidos en las directrices de la OCDE, si bien, realiza de los mismos un desarrollo más completo. Su objeto no es otro que armonizar las legislaciones nacionales, garantizando, en el territorio de cada uno de los Estados Miembros, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. En este sentido su ámbito de aplicación se orienta a los tratamientos de datos personales automatizados, sin perjuicio de lo cual los Estados Miembros podrán aplicar el Convenio a los datos de personas jurídicas y a los tratamientos manuales de datos, aunque tal circunstancia no se imponga en el Convenio.

Asimismo el Convenio recoge normas y principios que han sido incluidos tanto en la Directiva 95/46/CE como en la LOPD. Por un lado se establecen las obligaciones de implantar medidas de seguridad, la clasificación de datos especialmente protegidos y las normas relativas a las transferencias internacionales de datos y, por otro lado, se diseña una estructura de control, basada en dos niveles:

- Obligatoriedad de crear autoridades de control a nivel nacional con competencias que le permitan garantizar la aplicación de los principios del Convenio en el Derecho interno, cooperar con las restantes autoridades nacionales e intercambiar información.
- Creación de un Comité Consultivo en el que cada Estado Miembro designará a un representante y a un suplente, que tendrá como funciones:
  - Presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio.
  - Presentar propuestas de enmienda del presente Convenio, con arreglo al artículo 21.
  - Formular su opinión acerca de cualquier propuesta de enmienda al presente Convenio que se le someta, podrá, a petición de una Parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio.

En relación al Convenio 108 hemos de tener presente que con el transcurso de los años algunos de los aspectos contenidos en él han precisado de actualización, adoptándose el 8 de noviembre de 2001, un Protocolo Adicional al mismo con el objeto de adecuar el Convenio en la materias como los movimientos internacionales de datos.

3.3. La Directiva 95/46/CE

La Directiva es el reflejo de un proceso que ha ido teniendo lugar a lo largo de los años en los que se ha ido formando una "***conciencia europea sobre protección de datos***" conforme a la cual, los datos no son propiedad de quien los posee o los maneja, sino de su titular, del ciudadano, y solamente él tiene derecho a decidir quién, dónde, cuándo y cómo

los presenta al exterior, en el que ha adoptado carta de naturaleza el principio de la autodeterminación informativa[46].

Para comenzar con su exposición podemos hacer referencia a sus considerandos 7, 8 y 9:

«7. Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;

8. Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;

9. Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y

46 CONDE ORTIZ, C. (2005). *La protección de datos personales.* Dykinson.

sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;»

Con estos objetivos, el Consejo elaboró una Propuesta de Directiva, que tiene fecha de 27 de julio de 1990. Dicha Propuesta, a lo largo de su tramitación, sufrió diversas modificaciones, pero en todo caso adelantaba el propósito de la UE, armonizar las normativas de los países miembros en la materia con el objetivo principal de eliminar cualquier obstáculo a la circulación de datos de carácter personal y de conseguir un nivel aceptable y homogéneo de protección de los derechos de los ciudadanos en todo el territorio de la UE. Una vez recogidas todas las modificaciones, la Comisión presentó una "Propuesta modificada de Directiva 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".

3.3.1. Objetivos

Los objetivos perseguidos por la Directiva pueden resumirse en los siguientes:

- Aproximar y armonizar las disposiciones de los Estados Miembros sobre protección de la intimidad de las personas frente a la informática a través de una norma de carácter general.
- Promover a través de una "Directiva sectorial" una normativa sobre redes públicas digitales y de comunicaciones.
- Avanzar en la regulación necesaria para alcanzar un nivel de adecuado de Seguridad de los Sistemas de Información.

Es importante comprender que la Directiva es fundamental en la regulación actual de protección de datos, no solo en el ámbito europeo, sino también a nivel mundial, dado que las normas de la misma, en materia de transferencias internacionales de datos vienen a imponer un régimen básico al que deberán resultar “adecuados” los terceros Estados no

miembros de la UE, para que los datos puedan ser transmitidos libremente.

3.3.2. Ámbito

En cuanto al ámbito de aplicación de la norma, esta se extiende no solo a los tratamientos automatizados de datos, sino que también se incluye, de forma expresa a los tratamientos manuales tal y como establece su considerando 27:

«Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;»

Aparece pues la base para la generación de obligaciones referentes al control de los tratamientos realizados por medios no automatizados, fundamentalmente en papel. Aportación fundamental ya que en las primeras regulaciones de la materia el ámbito de aplicación se limitaba a los tratamientos automatizados.

3.3.3. Principales novedades

Además del ámbito de aplicación, las principales novedades aportadas por la Directiva pueden resumirse de la siguiente manera:

- Regulación del encargado del tratamiento.
- Desarrollo de los principios de calidad de los datos.
- Interés legítimo como legitimador del tratamiento.
- Introducción de una cláusula sobre la libertad de expresión.
- Reconocimiento del derecho de oposición.
- Reconocimiento de los derechos relacionados con las decisiones individuales automatizadas.
- Desarrollo de sistemas de autorregulación sectorial.
- Establecimiento de un régimen sistemático de las transferencias internacionales de datos.

Además, la Directiva implica un reforzamiento de las funciones de las autoridades de protección de datos y la creación del denominado Grupo del artículo 29. que, con carácter consultivo e independiente estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión y que tendrá los siguientes cometidos:

- Estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea.
- Emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros.
- Asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades.
- Emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

De esta forma, el **Grupo de Trabajo del Articulo 29 (GT29)**[47] ha venido ocupándose de forma continuada de los planes de la Unión Europea respecto a todas las materias

47 Pueden consultarse todos los documentos elaborados por el GT29 a través de la siguiente dirección: http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2 007_en.htm

relacionadas con la protección de datos de carácter personal y con su actividad ha sido un factor de impulso para el desarrollo de este marco normativo.

3.4. Transposición al ordenamiento jurídico español

La aprobación de la Directiva 95/46/CE y las obligaciones de transposición que de la misma se derivaban hicieron plantear la necesidad de modificar la entonces vigente LORTAD, opción que finalmente se desestimó, optándose por la aprobación de una nueva Ley Orgánica, la LOPD, que recoge lo exigido por la Directiva.

3.4.1. Directiva 2002/58/CE

La Directiva 2002/58/CE, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, denominada Directiva sobre la privacidad y las comunicaciones electrónicas deroga y sustituye la Directiva 97/66/CE, de 15 de diciembre.

La presente Directiva encaja por lo tanto con el interés existente en la UE por acelerar la introducción de las tecnologías digitales impulsando el desarrollo transfronterizo de los nuevos servicios de comunicaciones electrónicas, y garantizando la protección de los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios.

Se trata de la Directiva de referencia en el sector, regulando todo lo que se refiere tanto a los datos ligados a las telecomunicaciones tradicionales (tráfico, guías, etc.) como a las peculiaridades derivadas de la digitalización de las comunicaciones electrónicas, que generan nuevas formas de tratamientos (identificación de las líneas de llamada, desvío de llamada, etc.) así como nuevas categorías de datos, por ejemplo las anotaciones originadas por la conexión a la red y los archivos que recogen incidencias (archivos de logs y cookies) o los datos de localización[48].

48 CORRIPIO, M. R. (2002). *Novedades Legislativas sobre protección de datos. La Directiva 2002/58/CE*.

A nivel de su transposición al derecho español, la Directiva 2002/58/CE, hacía precisa una modificación del Real Decreto 1736/1998, de 31 de julio por el que se aprobó el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones. En este sentido, 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, derogó el RD 1736 e incorporó, entre otras las disposiciones exigidas por la Directiva 2002/58/CE.

3.4.2. Directiva 2006/24/CE

La presente Directiva[49], recoge la obligación de los proveedores de servicios de comunicaciones electrónicas de conservar los datos que permitan identificar el origen, el destino, la fecha, hora y duración de una comunicación electrónica, el tipo de comunicación realizada, el equipo utilizado y la localización de dicho equipo. La finalidad de esa conservación es que los datos puedan estar disponibles con fines de investigación, detección y enjuiciamiento de delitos graves.

Se trata de una norma dictada con el objeto de luchar contra el terrorismo y facilitar la protección de la seguridad nacional y seguridad pública, tal y como indica en su Considerando 7:

«Las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 destacan que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada»

Revista de Contratación Electrónica. Número. 32. Noviembre de 2002

49 La norma ha sido incluida en el ordenamiento jurídico español mediante la aprobación de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

3.5. Acuerdos y Autoridades Comunes de Control

Dentro del marco de protección de los datos personales hay que hacer una referencia a una serie de iniciativas tomadas dentro de este ámbito, que afectan directamente al objeto de nuestro estudio. Nos referimos a la participación de las siguientes Autoridades Comunes de Control:

- Europol
- Schengen
- Sistema de información aduanero
- Eurojust

3.5.1. Europol

La Oficina Europea de Policía (Europol), es el órgano encargado de facilitar las operaciones de lucha contra la criminalidad al seno de la UE. El Convenio Europol (Convenio basado en el artículo K.3 del Tratado de la UE, por el que se crea una Oficina Europea de Policía, hecho en Bruselas y que entró en vigor, de forma general y para España, el 1 de octubre de 1998) establece unos requisitos mínimos en materia de protección de datos personales que deberán cumplir los Estados Miembros que sean parte del mismo.

En concreto, cada Parte deberá adoptar las disposiciones nacionales necesarias para conseguir un nivel de protección de datos que sea, como mínimo, equivalente al resultante de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 (Convenio 108), teniendo en cuenta la Recomendación R(87) 15, de 17 de septiembre de 1987, del Comité de ministros del Consejo de Europa encaminada a regular la utilización de datos de carácter personal en el sector de la policía. Adicionalmente, en el artículo 24, se crea una Autoridad Común de Control independiente cuyo cometido será vigilar la actividad de Europol, con el objeto de garantizar que el almacenamiento, el tratamiento y la utilización

de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas y controlar la licitud de la transmisión de los datos que procedan de Europol. Esta Autoridad Común de Control estará integrada, como máximo, por dos miembros o representantes de las autoridades nacionales de control.

3.5.2. Schengen

El Acuerdo de Schengen, constituye uno de los pasos más importantes en la historia de la construcción de la UE. Tiene como objetivo finalizar con los controles fronterizos dentro del Espacio Schengen (formado por la mayoría de estados miembros de la Unión) y armonizar los controles fronterizos externos. Fue firmado el 14 de junio, 1985 en Schengen (Luxemburgo). Cinco estados[50] de la entonces Comunidad Económica Europea (CEE), llegaron a un acuerdo para la supresión de fronteras comunes. Posteriormente se han adherido otros 23 miembros.

En el Capítulo Tercero del Título IV del Convenio de Aplicación del Convenio de Schengen se establecen los principios y mecanismos destinados a garantizar una adecuada protección de los datos de carácter personal existentes en el SIS (Sistema de Información Schengen). En su artículo 114 figura que en cada país debe designarse una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre la parte nacional de ese sistema de información y de comprobar que el tratamiento y la utilización de los datos introducidos en el SIS no atentan contra los derechos de la persona que se trate. Asimismo, se indica que toda persona tendrá derecho a solicitar a esta autoridad que compruebe los datos referentes a ella integrados en él, así como el uso que se haga de los mismos. Para ejercitar este control, el artículo 115 del Convenio establece la creación de una Autoridad de Control Común encargada de desarrollar esas facultades sobre la unidad de apoyo técnico del SIS. La Autoridad de Control Común está compuesta por dos representantes de cada autoridad nacional de control. El artículo 10 del Real Decreto 428/1996, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, encomienda a ésta el ejercicio del control sobre el SIS y faculta al Director para nombrar a los dos representantes en la Autoridad de Control.

50 Alemania, Francia, Bélgica, Países Bajos y Luxemburgo

3.5.3. Sistema de Información Aduanero

Con el objetivo de contribuir a prevenir, investigar y perseguir las infracciones graves de las leyes nacionales en materia aduanera aumentado la eficacia de las administraciones aduaneras de los Estados miembros mediante la rápida difusión de información y la mejora de la cooperación entre las mismas, se estableció, mediante el Acto del Consejo 95/C 316/02, de 26 de julio de 1995 y en base al K.3 del Tratado de la Unión Europea, el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros. El también denominado Convenio SIA crea una Autoridad de Supervisión Común, con la finalidad de supervisar el funcionamiento del Sistema de Información Aduanero y examinar todas las dificultades de aplicación o interpretación que puedan surgir en su funcionamiento. La Agencia Española de protección de datos española está también representada en dicha autoridad.

3.5.4. Eurojust

El 28 de febrero de 2002, el Consejo de la Unión Europea aprobó una Decisión por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia organizada[51]. Los objetivos de Eurojust son fomentar y mejorar la coordinación, entre las autoridades competentes de los Estados miembros, de las investigaciones y actuaciones judiciales en marcha, en particular, facilitando la ejecución de la asistencia internacional judicial y de las solicitudes de extradición y, con carácter general, apoyando a las autoridades competentes de los Estados miembros para dar mayor eficacia a sus investigaciones.

Además, la Decisión Eurojust establece una Autoridad Común de Control de la que forma parte el Director de la Agencia Española de Protección de Datos y cuyo reglamento fue aprobado el 2 de marzo de 2004[52]

51 Diario Oficial de la Unión Europea (2002). Serie L. Decisión del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia. Número 63. Marzo de 2002.

52 Diario Oficial de la Unión Europea. Serie C. Acto de la Autoridad Común de Control de Eurojust de 2 de marzo de 2004 por el que se establece su Reglamento interno. Número 86. Abril de 2004.

4. El marco español

4.1. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

4.1.1. Antecedentes

El antecedente directo de la Ley Orgánica de Protección de Datos es la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD)[53]. Se trata de una norma dictada en desarrollo el artículo 18 de la Constitución Española de 1978, que recogía un concepto de privacidad que pretendió ir más allá de la protección de la intimidad de la persona:

«Un conjunto más amplio, más global, de facetas de su personalidad que aisladamente consideradas pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado»

Por tanto, la LORTAD pretende *«delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley».*

Por tanto, el objetivo principal de la LORTAD es la limitación del uso de la informática y otros medios de tratamiento automatizados, en aras de la protección del derecho al honor, la intimidad y la propia imagen, siendo su ámbito de aplicación delimitado a los ficheros

53 Jefatura del Estado. *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*. Publicada en el Boletín Oficial del Estado número 262 de 31 de octubre de 1992

automatizados o bases de datos tratadas por medios informáticos.

Con este antecedente, en 1999 se aprueba la actual **Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD)**, norma que deroga a la LORTAD y que tiene como finalidad principal, transponer a la normativa nacional 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 esos datos. Una de sus principales novedades es incluir, en su ámbito de aplicación, los ficheros no automatizados, centrando toda su protección en el tratamiento de datos de carácter personal sea cual sea el soporte o medio de su tratamiento, con el fin de proteger los derechos fundamentales y libertades públicas de los ciudadanos.

4.1.2. Objeto

La LOPD tiene como objeto *«garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor en intimidad personal y familiar»*

Se han provocado variados debates acerca de cuál es el bien jurídico protegido en concreto, esto es, cuales son los derechos de la persona que protege la LOPD, libertades públicas, privacidad, intimidad, derechos fundamentales, etc., pero de lo que no cabe duda es que únicamente caen bajo la tutela de la los titulares de dichos datos, siempre que se trate de personas físicas. No obstante, esta conclusión que parece obvia no ha dejado de provocar cuestiones acerca de su aplicación práctica, por ejemplo, respecto a los datos de los empresarios individuales, autónomos y profesionales. Este es un extremo que el Reglamento de desarrollo de la LOPD ha tenido que aclarar, pese a que la Agencia Española de Protección de Datos ya se había pronunciado sobre este punto en diversas ocasiones.

En lo relativo al objeto de la LOPD, éste se ajusta al concepto del denominado *Habeas Data*, o *«control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar, en último extremo, el libre*

desarrollo de nuestra personalidad"[54], concepto identificado con la denominada *"Autodeterminación Informativa" o "Libertad Informática"*.

4.1.3.• Ámbito de aplicación

El ámbito de aplicación de la LOPD se encuentra definido en su artículo 2:

«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».

Continúa el citado artículo en los siguientes términos:

«Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando el responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional Público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito».

En cuanto a los ficheros excluidos del ámbito de la LOPD, la norma determina su ámbito de aplicación de la ley por exclusión, esto es, por la referencia a los ficheros que no se hallan sujetos al ámbito de aplicación de la Ley, y así a tenor de su artículo 2.2 se establece

54 MURILLO DE LA CUEVA. P. L. (1990). *El Derecho a la Autodeterminación Informativa. La Protección de Datos Personales frente al Uso de la Informática*. TECNOS. Madrid.

que la LOPD no será de aplicación:

«a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos».

Además, la LOPD recoge también una serie de ficheros que se regirán por sus disposiciones específicas:

«3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

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

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

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

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

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.»

4.2. El Reglamento de Desarrollo de la LOPD

4.2.1. Antecedentes

La LOPD adaptó nuestro ordenamiento a lo dispuesto por 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. A fin de garantizar la seguridad jurídica la Ley declaró subsistentes las normas reglamentarias existentes y, en especial:

- RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos
- RD 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal.
- RD 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

De forma adicional, habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999. Por otra parte, desde la publicación en 1992 de la LORTAD, dos textos legales habían atribuido competencias adicionales a la Agencia Española de de Protección de Datos y dichas competencias debían ser incorporadas a la normativa vigente. Nos referimos a la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Con este desarrollo normativo se vio la necesidad de desarrollar lo que acabó denominándose "*Nuevo Reglamento*" y que finalmente se aprobó mediante el Real Decreto 1720/2007, de 21 de diciembre.

4.2.2. Objeto

El artículo 1 del Reglamento define su objeto en los siguientes términos:

«1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.»

4.2.3. Ámbito de aplicación

El Reglamento, en lo que al ámbito de aplicación se refiere, viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio y que han sido derogados por el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.

Tal y como establece el artículo 2 de la LOPD, el ámbito de aplicación queda establecido de la siguiente manera:

*«**Artículo 2. Ámbito de aplicación.***

1. 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.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional

público.

Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

Los ficheros regulados por la legislación de régimen electoral.

Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

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

Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras

por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.»

4.3. La Agencia Española de Protección de Datos y otros Organismos de Control. Regulación específica

4.3.1. Antecedentes

Uno de sus primeros antecedentes lo encontramos en la LORTAD, que dedicaba su título IV a su regulación y que en su artículo 34 creaba este Ente de Derecho Público:

«1. Se crea la Agencia de Protección de Datos.

2. La Agencia de Protección de Datos es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio que será aprobado por el Gobierno, así como por aquellas disposiciones que le sean aplicables en virtud del artículo 6.5 de la Ley General Presupuestaria».

Más tarde, la Directiva 95/46/CE, venía a reconocer su importancia y en sus Considerandos 62 y 63 establecía:

«62. Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;

63. Considerando que dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa;

4.3.2. Regulación actual

La LOPD adaptando el contenido de la Directiva, siguió la misma estructura utilizada ya en la LORTAD a este respecto, y dedica también su Título VI (artículos 35 a 41) a la regulación de la Agencia como un Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada. La Agencia Española de Protección de Datos actúa por lo tanto con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Por otra parte, el artículo 41 LOPD, se ocupa de las Agencias Autonómicas en los siguientes términos:

«1. Las funciones de la Agencia Española de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j, k y l, y en los apartados f y g en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.»

En este sentido, hasta la fecha se han creado tres: Cataluña[55], Madrid[56] y País Vasco[57].

55 Presidencia de la Generalidad de Cataluña. *Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos*. Publicado en el Diario Oficial de la Generalidad de Cataluña número 3625, de 29 de abril de 2002

56 Secretaría General Técnica de Vicepresidencia, Consejería de Cultura y Deporte y Portavocía del Gobierno. *Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid*. Publicada en el Boletín Oficial de la Comunidad de Madrid, de 25 de julio de 2001.

57 Presidencia del Gobierno. *Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.* Publicado en el Boletín Oficial del País Vasco número 44, de 04 de marzo de 2004

4.3.3. Instrucciones, de la Agencia Española de Protección de Datos

El artículo 37 LOPD, recoge las funciones de la Agencia, entre las cuales, podemos destacar las siguientes:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
- Dictar las instrucciones precisas para adecuar los tratamientos a los principios de la Ley.
- Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

En lo relativo a las **Instrucciones** el artículo 37.1.c) de la LOPD incluye, entre las funciones de la Agencia, la de *«dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley»*

En cumplimiento de esta previsión, la Agencia ha ido desarrollando una serie de instrucciones en aquellos casos en los que se ha considerado que las previsiones de la Ley no eran lo suficientemente clarificadoras para los responsables de los tratamientos. Muchas de las Instrucciones han sido posteriormente consideradas a la hora de desarrollos posteriores. Este ha sido el caso del Reglamento de Desarrollo de la LOPD, que ha recogido, entre otros, aspectos contenidos en la Instrucción 1/998.

4.4. Otra normativa relacionada

Vamos a terminar la referencia al marco normativo español con la mención de otras normas que si bien no regulan directamente la protección de los datos de carácter personal, si se

encuentran, en razón de su objeto, directamente relacionadas.

4.4.1. Ley 34/2002, de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI)

La presente Ley que tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado Interior (Directiva sobre el comercio electrónico). Incorpora también parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

La Ley pretende solventar las incertidumbres jurídicas, que el avance de la Sociedad de la Información ha implicado, estableciendo un marco jurídico adecuado, capaz de generar en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio. En lo que atañe a la protección de datos personales, la LSSI afecta a la materia en diferentes aspectos, regulando:

- Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.
- Comunicaciones comerciales electrónicas.
- Nuevas competencias sancionadoras de la Agencia los supuestos delimitados por el artículo 43 LSSI.

4.4.2. Ley 32/2003, General de Telecomunicaciones (LGT)

Entre sus objetivos está el de defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de comunicaciones electrónicas en adecuadas condiciones de elección, precio y calidad, y salvaguardar, en la prestación de éstos, la vigencia de los imperativos constitucionales, en particular, el de no discriminación, el del respeto a los derechos al honor, a la intimidad, a la protección de los datos personales y al secreto en las comunicaciones. Con esta finalidad dedica el Capítulo III del Título III al *"Secreto de las*

comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas". Por último, y en el mismo sentido que la LSSI, la LGT prevé la atribución de competencias sancionadoras a la Agencia.

4.4.3. Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen

Desarrolla el artículo 18 de la Constitución Española, dotando de protección civil a los denominados derechos fundamentales de la personalidad. El ámbito de protección establecido por la norma se extiende por lo tanto a aspectos estrechamente relacionados con el derecho a la protección de datos de carácter personal de forma que en muchas ocasiones, los tratamientos de datos deberán analizarse también desde la perspectiva de posibles intromisiones en el honor, la intimidad o la propia imagen pudiendo las personas agraviadas ejercer con esta base las acciones civiles pertinentes ante este orden jurisdiccional.

4.4.4. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Delitos informáticos

Dentro de los denominados *"delitos informáticos"*, afectan especialmente al objeto de nuestro estudio los ataques contra el derecho a la intimidad, entre los que se encuentran los delitos de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos (artículos 197 al 201 del Código Penal). Las conductas tipificadas son, entre otras:

- Descubrimiento de secretos o vulneración de la intimidad de otro, sin su consentimiento, mediante el apoderamiento de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales.
- Interceptación de telecomunicaciones o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.
- Acceso, alteración, apoderamiento, utilización, modificación, en perjuicio de tercero, de datos reservados de carácter "personal o familiar" que se hallen

registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

- Difusión, revelación o cesión a terceros de los datos referidos en el punto anterior.

4.4.5. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Incorpora al ordenamiento español la Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. La Ley establece los datos que deben conservarse, incluyendo todos los exigidos por la Directiva en su artículo 3 y ampliándolos como en los casos de los servicios suplementarios o de los servicios de mensajería o multimedia.

4.4.6. Normativa adicional

No podemos olvidar que existen otras muchas normas que aluden de forma más o más o menos relevante a la protección de datos personales y que, por lo tanto, forman parte del marco normativo que estamos analizando. Por tanto se hace necesario incluir una referencia a las que entendemos más importantes desde este punto de vista:

- Ley Orgánica 4/1997 por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos
- Ley Orgánica 10/2007 Reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN
- Ley Orgánica 4/1997 Por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos
- Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información
- Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos
- Real Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
- Ley 44/2006, de mejora de la protección de los consumidores y usuarios

- Ley 59/2003, de Firma Electrónica
- Real Decreto 1553/2005, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
- Real Decreto 209/2003, por el que se regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos
- Real Decreto 424/2005, por al 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
- Real Decreto 1736/1998, que aprueba el Reglamento que desarrolla el Título III de la Ley General de Telecomunicaciones.
- Orden CTE 771/2002, que establece las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.

5. La protección de datos en derecho comparado

En este punto conviene analizar, siquiera de forma breve, el estado de la protección de los datos de carácter personal en los países de nuestro entorno. El objetivo de este breve análisis no es otro que:

- Analizar el nivel de protección y de desarrollo normativo alcanzados en España, poniéndolos en relación con la situación verificada en otros países cercanos.
- Conocer las forma de regular el derecho a la protección de datos personales que se han dado en otros estados
- Estudiar aspectos relativos al derecho comparado en este ámbito que serán

relevantes para el estudio de la problemática implícita en las Transferencias Internacionales de Datos.

Analizaremos los casos de Francia, como ejemplo de país de nuestro entorno en el marco de la UE, EEUU e incluiremos una referencia general a los países Iberoamericanos, haciendo especial mención a dos casos significativos: Argentina y Uruguay.

5.1. Francia

Francia ha sido uno de los países pioneros en la protección de datos de carácter personal. La ley *"Informática y Libertades"*, cuyos primeros trabajos de preparación datan de 1974, es una de las más antiguas en el ámbito de la protección de los datos personales. En 1974 se dio a conocer un proyecto gubernamental de interconexión de todos los ficheros administrativos, en base a un número de identificación único para cada ciudadano (conocido bajo el nombre de proyecto **SAFARI**). Con este objeto se constituyó una comisión encargada de hacer propuestas a fin de garantizar que el desarrollo de la informática no permitiera intromisiones en la vida privada, y las libertades individuales de los ciudadanos.

La Ley fue finalmente aprobada el 6 de enero de 1978. Naturalmente el desarrollo posterior de la protección de los datos personales en Francia se ha realizado conforme a las pautas marcadas a nivel europeo, si bien hay que señalar que Francia fue el último país de la UE en transponer el contenido de la Directiva 95/46/CE, con una ley de 6 de agosto de 2004 que modificó profundamente la ley de 6 de enero de 1978. Este retraso, justificado en parte por el hecho de que la Ley de 1978 cubría en su mayor parte el contenido de la Directiva, ha traído como consecuencia una de las leyes más modernas del continente, que sacó provecho de todas las opciones abiertas por la directiva para transformar su manera de enfocar la protección de los datos personales y de poner en práctica sus principios. Es de destacar en este sentido, la atribución de responsabilidad de las empresas en la aplicación de la Ley (reconociendo la importancia de la autorregulación en este campo), pero también la de los ciudadanos en la protección de sus derechos.

Asimismo se han tenido en cuenta todas las posibilidades de simplificación de algunos

procesos y se introducido lo que en este país fue una novedad: la potestad sancionadora de la Autoridad de Control. En aras de procurar un equilibrio en el control de los tratamientos, no limitándolos exclusivamente a un control previo a su registro por parte de la CNIL (Comisión Nacional de Informática y Libertades, se han desarrollado medidas de control posterior siendo especialmente significativo el establecimiento de la potestad sancionadora de la CNIL. Hasta la aprobación de la reforma de 2004, la CNIL no tenía potestad de sancionar directamente los responsables de tratamientos que infringían la ley "*informática y libertades*". A cambio, siempre ha existido en el derecho francés infracciones y sanciones penales correspondientes en materia de protección de datos personales, y de hecho, esta posibilidad se mantiene abierta en el nuevo marco legislativo.

Conforme a este diseño, la CNIL siempre ha tenido la facultad de denunciar al Ministerio Fiscal las infracciones de las que tenía conocimiento en el ejercicio de sus funciones. También podía dirigir apercibimientos que hacía públicos. La Ley de 6 de agosto de 2004, de acuerdo con la idea recogida en la Directiva, ha otorgado a la CNIL una potestad sancionadora propia: la facultad de infligir multas, de un importe de hasta 300.000 € en caso de reincidencia.

En este sentido, la historia del desarrollo de la protección de datos en Francia, como en el resto de los Estados Miembros de la Unión Europea, es la de la convergencia hacia un modelo común cuya referencia actual es la Directiva 95/46/CE. Esta capacidad de estandarización es sin duda el gran logro de la Unión en este terreno.

5.2. Estados Unidos

El problema inicial para el análisis de la regulación en los Estados Unidos se basa en el hecho de que no existe, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad, sino a lo sumo normas dispersas aplicables a sectores muy concretos. La protección de la intimidad y de los datos personales en Estados Unidos se enmarca en un entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial. La Ley de Privacidad data de 31 de diciembre de 1974, aunque en la actualidad, y debido a la dinámica y flexibilidad que las nuevas tecnologías de la información imponen a la

sociedad, ha sido ya modificada en varias ocasiones. En su Exposición de Motivos, se recoge la siguiente declaración:

«El Congreso estima que la privacidad del individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales (…) el creciente uso de ordenadores y de una tecnología compleja de la información, si bien es esencial para el eficiente funcionamiento de las Administraciones Públicas, ha aumentado grandemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal.»

No obstante, EEUU no tiene desarrollada una ley de protección de datos de la forma y con el alcance que existe en todos los estados miembros de la Unión Europea. Por el contrario, EEUU protege los datos de carácter personal de una forma indirecta y precisamente , este es un problema que se encuentra en discusión en la actualidad debido al desequilibrio existente cuando se realizan transferencias internacionales de datos de ciudadanos de la UE a otros países, debido a que se puede perder el nivel de protección deseado. Naturalmente la regulación es prolija y ha ido evolucionando a lo largo de los años. Algunos de los principales hitos son:

- **Public Law 93-579, de 31 de diciembre de 1974. Privacy Act**
- **The Tax Reform Act (1978)**. Sobre la confidencialidad de los datos bancarios
- **The Electronic Fund Transfer Act (1978)**. Sobre la obligación de las instituciones financieras que efectúen transferencias electrónicas u otros servicios bancarios por ese procedimiento, de informar a sus clientes del acceso de terceras personas a sus bancos de datos
- **Electronic Communications Privacy Act (1986)**. Responde a las necesidades de defensa de la privacidad en las nuevas formas de comunicación. Prohíbe la interceptación de mensajes mandados por medio de esta tecnología, define todo lo relativo a comunicaciones electrónicas (correo electrónico, transmisiones vía satélite, telefonía celular, etc.), establece las sanciones civiles y penales por infringir la normativa, etc.
- **The Computer Security Act (1986)**. Regulación para la protección de los Sistemas de Información y Criptografía del Gobierno de los EEUU

- **The Computer Matching and Privacy (1988)**. Regulación para prevenir el excesivo desarrollo que se estaba produciendo en la elaboración de dossiers automatizados, y por lo tanto el más que probable intercambio de datos personales entre las compañías sobre todo del sector privado
- **Social Security On-line Privacy Protection Act (1997)**. Carta que prohíbe el acceso a los datos de Seguridad Social, ingresos y beneficios a través de Internet sin el consentimiento escrito del titular
- **Personal Information Privacy Act (1997)**. Carta para proteger la privacidad de los individuos respecto al número de la Seguridad Social y a otra información personal
- **Federal Internet Privacy Protection Act (1997)**. Regulación que prohíbe a las agencias del Gobierno habilitar información confidencial referente a personas a través de Internet

Como vemos, la protección de la intimidad y de los datos en Estados Unidos se enmarca en un entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial.

5.2.1. El Acuerdo de Puerto Seguro

Los EEUU iniciaron en 1999 negociaciones con la Unión Europea en orden a conseguir una declaración de adecuación del nivel de protección de datos personales. Esta declaración tiene como punto de partida, el estudio de la legislación de protección de datos aplicable en todo el territorio del estado solicitante y como hemos visto, el problema inicial, se centra en el hecho de que no existe, dado el marcado carácter autorregulador del comercio en dicho país, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad, sino a lo sumo normas dispersas aplicables a sectores muy concretos. A fin de superar los problemas derivados de la dispersión normativa, el Departamento de Comercio de los EEUU presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea emitió un borrador de "*principios de puerto seguro*", a fin de garantizar a los operadores que se adhirieran a los mismos una "*presunción de adecuación*" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores.

Para ello, aquéllos debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas. El Acuerdo de "Puerto Seguro" consta de siete principios básicos:

- Notificación (información a los afectados).
- Opción (posibilidad de oposición de los afectados).
- Transferencia ulterior a terceras empresas.
- Seguridad.
- Integridad de los datos (principios de finalidad y proporcionalidad).
- Derecho de acceso.
- Aplicación (procedimientos para la satisfacción de los derechos de los afectados).

La Comisión Europea, mediante su Decisión de 26 de Julio de 2000[58], y con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, se pronunció sobre la adecuación conferida por los principios de puerto seguro publicados por el Departamento de Comercio de EEUU.

5.2.2. Transmisión de Datos de Pasajeros (PNR) a EEUU

Tras los atentados terroristas del 11 de septiembre de 2001, los Estados Unidos adoptaron una normativa (*Patriot Act*) por la cual las compañías aéreas que operen rutas con destino u origen en EEUU o atraviesen su territorio deben facilitar a las autoridades estadounidenses el acceso electrónico a toda una serie datos contenidos en sus sistemas de reservas y de control de salidas, denominados *Passenger Name Records* (PNR). La Comisión Europea, tratándose de un requerimiento cuya incidencia en los datos personales de los viajeros podría suponer la vulneración de las normas comunitarias y de los Estados miembros en materia de protección de datos, decidió iniciar negociaciones con las autoridades americanas con vistas a minimizar sus efectos.

58 Comisión de las Comunidades Europeas. *Decisión de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América*. Publicada el 25 de agosto de 2000 en el Diario Oficial de las Comunidades Europeas, número L 215

Estas negociaciones culminaron en mayo de 2004 con la Decisión 2004/535/CE[59], por la que la Comisión Europea declaraba que el nivel de protección de datos que otorgarían las autoridades americanas a los datos que le fueran transmitidos era considerado adecuado desde el punto de vista de la normativa comunitaria; un requisito, por otra parte, indispensable a la hora de realizar transmisiones de datos a países terceros. Por su parte, y con objeto de otorgar una base jurídica a las transmisiones de datos por parte de las compañías aéreas, el Consejo de la Unión Europea aprobó, a través de la Decisión 2004/496/CE[60], la celebración de un Acuerdo entre la Comunidad Europea y EEUU al respecto.

5.3. Protección de Datos en Iberoamérica

Se trata de un ámbito muy amplio y heterogéneo, en el que la protección de los tratamientos de datos personales ha sido regulada en función del nivel de desarrollo de la Sociedad de la Información alcanzado en cada caso y siendo, en todo caso, un desarrollo relativo. En el año 2004, y según la Unión Internacional de Telecomunicaciones, en América Central y del Sur, aproximadamente unos 47 millones de habitantes tenían acceso a Internet con un promedio de crecimiento que para el periodo de 2000 a 2004 era del 271%. Realizaremos en primer lugar una primera aproximación a las tendencias que se desprenden del estudio de los diferentes modelos legislativos adoptados y posteriormente

59 Comisión de las Comunidades Europeas. *Decisión de la Comisión de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection).* Publicada el 6 de julio de 2004 en el Diario Oficial de las Comunidades Europeas, número L 235

60 Comisión de las Comunidades Europeas. *Decisión del Consejo de 17 de mayo de 2004 relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos.* Publicada el 20 de mayo de 2004 en el Diario Oficial de las Comunidades Europeas, número L 183

nos referiremos al estado de la cuestión en países concretos.

5.3.1. Aproximación general a la regulación de la protección de datos de carácter personal en Iberoamérica

Iberoamérica no tiene una tradición tan arraigada en materia de protección de datos personales como podamos encontrar en Europa o Estados Unidos. Esto es consecuencia directa, de una parte, del escaso nivel de desarrollo que las Tecnologías de la Información alcanzaron en estos países, sobre todo en las décadas de los 70 y 80, años en los que, como hemos visto, en Europa se estaba formando la que hemos denominado "*conciencia de protección de datos*". Por otra parte, este factor en algunos casos combinó con la existencia de regímenes totalitarios poco receptivos al reconocimiento de los derechos fundamentales que sirvieron como base para desarrollar el derecho a la protección de datos personales.

Esta situación comenzó a cambiar hacia finales de la década de los ochenta, cuando empezaron a surgir voces exigiendo protección en este ámbito. En este sentido, fue la Constitución Brasileña de 1988, el primer texto fundamental que reguló la materia adoptando un procedimiento basado en la acción del "**Habeas Data**". Se trataba de una acción concebida como una protección constitucional contra los abusos del poder y las ilegalidades cometidas por los administradores y encargados de gestionar datos personales para los poderes públicos. A través de la acción de Habeas Data, los interesados pueden solicitar la exhibición de sus datos personales a la autoridad responsable de su registro y si fuere procedente, exigir su supresión, rectificación o actualización. En concordancia con este primer antecedente, "Habeas Data" es la denominación que mejor representa a los temas de protección de datos personales en Iberoamérica, coloquialmente hablando, si bien desde un punto de vista estrictamente técnico con este término nos estamos refiriendo a una garantía procesal constitucional. El Habeas Data fue posteriormente adoptado por otras constituciones como es el caso de Argentina, Perú, Paraguay y Ecuador.

Como señala, Fernando Argüello Téllez[61], su objeto y ámbito de aplicación han sido

61 PIÑAR MAÑAS, J.L. (2006). *Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal*. En Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch/Agencia Española de Protección de Datos/Red Iberoamericana de Protección de Datos.

redactados de diversas maneras: mientras que en algunos países su alcance está limitado a los ficheros de titularidad pública, en otros se garantiza también el acceso a ficheros de titularidad privada; en cuanto al ámbito de la protección, normalmente no se hace distinción en cuanto a que los tratamientos estén automatizados o no. En términos generales, el Habeas Data es un procedimiento abreviado, para el que se establecen plazos cortos. Su tramitación es competencia de los órganos de justicia. De todas formas, y examinando el Habeas Data desde la perspectiva del nivel de protección que establece la Directiva, debe entenderse que, en general, nos encontramos ante un procedimiento que no garantiza un nivel de protección comparable.

En efecto, se trata de procedimientos diseñados para "*corregir*" irregularidades en el tratamiento de datos personales, pero no es el método idóneo para prevenir acciones lesivas para los derechos de las personas, y desde luego no permite conocer la forma en la que los tratamientos deben realizarse. En este sentido, si tenemos en cuenta los requisitos establecidos por el GT29 en el documento WP 5025/98, "*Transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de Datos de la UE"***,** nos damos cuenta de que, entre todos los puntos exigidos por la UE, el procedimiento descrito solo cumple con el requisito de cumplir con el derecho de acceso y rectificación. No obstante, como decimos, la situación no es homogénea. Por otra parte, aparecen en este sentido dos tendencias opuestas. De un lado los países que han optado por leyes "*verticales*", esto es, cuyo objeto se atiene exclusivamente a cierto tipo de datos, en general comerciales o relacionados con operaciones de crédito. Se trata de una forma de legislar cuyo origen podemos establecer en la ley 27.489 de Perú, de junio de 2001, por la que se regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información. Posteriormente, a esta opción se adscribieron otros estados como Paraguay (2001), México (2002), Panamá (2002) y Uruguay (2004). Todos ellos aprobaron leyes que regulan únicamente los llamados datos crediticios rechazando la opción de usar un modelo horizontal, a imagen del europeo en desarrollo de la Directiva 95/46/CE. De otro lado, encontramos países que han aprobado leyes "*horizontales*", entre los que podemos citar Argentina, Chile, y otros países cuyo desarrollo parece también más adecuado, si bien se ha producido a un ritmo más lento. Nos referimos a Brasil, México y Colombia.

Como, cabe afirmar que si bien, el desarrollo normativo se está produciendo a un ritmo

más lento que en Europa, hay que valorar que el punto de partida es diferente y el hecho de que en los últimos años se está produciendo un notable avance en este sentido. El hecho señalado de que en muchos países se esté llevando a cabo una regulación "*vertical*", puede hacer pensar que el legislador Iberoamericano no valora adecuadamente importancia y necesidad de proteger adecuadamente el derecho fundamental de la protección de datos. Por el contrario, encontramos que, si bien motivos generalmente políticos llevan a optar por regulaciones de este tipo, estas normas suelen ofrecer un nivel de protección limitado en su ámbito de aplicación pero muy avanzado.

5.3.2. La Red Iberoamericana de Protección de Datos

En junio de 2003, en el marco del Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua (Guatemala), y a iniciativa de la Agencia Española de Protección de Datos, se creó la Red Iberoamericana de Protección de Datos. La idea consistía en la creación un foro abierto a la incorporación de los países iberoamericanos, con el propósito de potenciar las iniciativas de intercambio de experiencia entre los miembros y de reforzar la colaboración en materia de protección de datos. En noviembre del mismo año, la Declaración de Santa Cruz de la Sierra (Bolivia), firmada tras la XIII Cumbre de Jefes de Estado y de Gobierno de Iberoamérica, recogió en su artículo 45 el reconocimiento expreso de la protección de datos como derecho fundamental y la labor de la Red Iberoamericana. En estos momentos, la Red cuenta con la representación de entidades de control de 17 países.

Entre los objetivos de la Red destaca el impulso para la elaboración de los instrumentos normativos necesarios para garantizar la protección del derecho a la protección de datos personales en aquellos países de la Comunidad Iberoamericana que aún no hayan afrontado su regulación. Se trata de una tarea importante, teniendo en cuenta que debe permitir el desarrollo homogéneo en este marco, igualando las diferencias que de otra forma podrían surgir entre los niveles de protección que de otra forma, supondrían un obstáculo para la transmisión de dichos datos y por lo tanto, para el ejercicio de actividades económicas. Con este fin, la Red lleva a cabo múltiples actividades entre la que destaca la celebración de encuentros anuales en los que sus miembros participan activamente intercambiando experiencias y debatiendo acerca de las novedades que se van produciendo en la materia.

La Red Iberoamericana de Protección de Datos es por lo tanto un importante instrumento destinado a facilitar la homogeneización y el desarrollo de la normativa sectorial entre los países miembros.

5.3.3. Uruguay

En el año 2004 la República Oriental del Uruguay reguló la acción de Habeas Data tras un proceso que ha durado siete años. La norma contiene además un estatuto de datos personales crediticios que implicó la mitad del debate parlamentario (cuatro años). En el artículo 2 de esta Ley, se puede leer:

«Se exceptúan de esta ley, el tratamiento de datos que no sean de carácter comercial como por ejemplo: a) datos de carácter personal que se originen en el ejercicio de las libertades de emitir opinión y de informar... y b) datos sensibles sobre la privacidad de las personas, entendiéndose por éstos, aquellos datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical...»

Nos encontramos ante un caso típico de la tendencia comentada a la aprobación de Leyes "*verticales*". Se ha interpretado la opción por este tipo de regulación como una forma de evitar que el Habeas Data pueda ser utilizado para recabar la información gestionada por el Estado en relación con actuaciones llevadas a cabo en periodos anteriores. De hecho, este caso se dio en Argentina donde, en 1998, en el caso Urteaga, se permitió al hermano de un desaparecido el acceso a toda información relativa a la desaparición.

5.3.4. Argentina

Dentro de la doble perspectiva que hemos visto que afecta a la regulación de la materia en los países analizados, Argentina, ha desarrollado una protección de datos personales mediante leyes generales y sectoriales, todas ellas de efecto jurídico obligatorio. Las normas generales están contempladas en la Constitución, la Ley 25 326 sobre protección de datos personales y el Decreto Reglamentario nº 1558/2001.

La Constitución argentina prevé un recurso judicial de Habeas Data. Se trata como hemos visto de una subcategoría del procedimiento contemplado en la Constitución para proteger los derechos constitucionales y, por tanto, eleva la protección de datos personales a la categoría de derecho fundamental. De conformidad con el tercer párrafo del artículo 43 de la Constitución, toda persona podrá interponer esta acción (Habeas Data) para tomar conocimiento de los datos que se refieren a ella y de su finalidad que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá vulnerarse el secreto de las fuentes de información periodística. La jurisprudencia argentina ha reconocido el Habeas Data como un derecho fundamental y directamente aplicable.

La Ley 25 326 sobre protección de datos personales, de 4 de octubre de 2000 desarrolla y amplía lo dispuesto en la Constitución. Contiene normas sobre los principios generales de protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial Habeas Data.

El Decreto Reglamentario número 1558/2001, de 3 de diciembre de 2001 introduce las normas de aplicación de la Ley, completa lo dispuesto en ella y clarifica aspectos de la Ley que podrían interpretarse de manera divergente.

Además de la ley y el reglamento comentados, tres disposiciones sostienen la protección de datos en Argentina:

- Clasificación de infracciones y la graduación de las sanciones" (Disposición 1/2003 BO 30/06/2003).
- Registro Nacional de Bases de Datos (Disposición 2/2003 BO 27/11/2003).
- Disposición 1/2004 BO 26/02/2004, conforme al cual se llevó a cabo el primer censo nacional de archivos, registros, bases o bancos de datos privados. con carácter obligatorio.

A la vista de la normativa comentada, cabe afirmar que la legislación argentina cubre la

protección de los datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos públicos y la protección de datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos privados «destinados a dar informes», incluidos «*aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito*». Por este motivo, en junio de 2003, Argentina alcanzó la declaración de país con nivel de protección adecuado por parte de la Unión Europea. El GT29 coronaba de esta forma el proceso de legislativo necesario para una protección adecuada de los datos personales:

«A efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, se considera que Argentina garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad»

En resumen, estamos en presencia, de una de las legislaciones más avanzadas en la materia dentro de los países de su entorno.

IV. CONCLUSIONES

De todo lo analizado con anterioridad conviene extraer las siguientes con conclusiones:

- Hay que resaltar la forma en la que la regulación de este derecho ha ido siguiendo un proceso de estandarización siendo esto especialmente significativo en el ámbito de la UE. La tendencia es sin duda a la unificación y ello derivará por un lado en una mejora de la protección de los derechos fundamentales de los ciudadanos, pero también en la garantía de que esta protección no interferirá en los flujos de información que cada vez en un mayor volumen son la base de la actividad económica a nivel global.
- Amplitud de un marco normativo que afecta a un número creciente de áreas. La protección de datos personales es un factor a tener en cuenta en sectores tan dispares como las Telecomunicaciones, la Seguridad, las Administraciones Públicas, los Servicios Sanitarios, etc.

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

I. ÁMBITO OBJETIVO

1. Introducción

En este punto del discurso nos centraremos en el análisis del ámbito comprendido en el régimen jurídico de protección y específicamente, cual es el ámbito abarcado por la LOPD. Comprobaremos como lo esencial para determinar el ámbito objetivo de aplicación de la LOPD es que nos encontremos ante datos personales que formen parte, o estén en disposición de formar parte, de un fichero de datos personales y que los mismos sean objeto de tratamiento.

Nos centraremos en el análisis de tres conceptos: dato personal, fichero y tratamiento, para, de una forma posterior detallar cual es el ámbito subjetivo de aplicación, esto es, qué personas están sujetas por las obligaciones contenidas en la LOPD y cuales son los casos especiales que debemos conocer para llevar a cabo una aplicación adecuada de la normativa.

2. Ámbito objetivo de aplicación

Tal y como establece el artículo 2 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».*

Por tanto debemos entender que el estudio del ámbito objetivo de aplicación de la normativa en materia de protección de datos de carácter personal, debemos detenernos en tres conceptos fundamentales: dato personal, fichero y tratamiento.

Entendemos por "*dato personal*" toda información relativa a personas físicas identificadas o identificables. Por tanto debemos entender que la protección de los datos personales se refiere exclusivamente a la privacidad e intimidad de las personas físicas, pero no de las personas jurídicas. Además, otro concepto clave en la definición de dato personal es que el mismo nos proporcione una información acerca de la persona a la que se refiere, y que exista una asociación entre la información proporcionada y el interesado. La asociación entre la información referida a una persona física y dicha persona en concreto es el aspecto determinante para que podamos afirmar la

existencia de un dato personal a los efectos de nuestro régimen jurídico.

En relación al concepto "*fichero*" debemos decir que sobre él recaen gran parte de las obligaciones que fija la normativa en la materia. Un fichero es un conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. De esta definición podemos extraer que si bien existe la necesidad de una organización u ordenación de los datos, por contra, no se requiere que el fichero esté automatizado.

Para finalizar, cuando hablamos de *"tratamiento de datos personales"* nos estamos refiriendo a cualquier operación o procedimiento técnico, sea o no automatizado, que permita, entre otras cosas, la recogida, conservación, modificación, consulta, o cancelación de estos datos. En este sentido tomaremos como referencia la clasificación propuesta por Davara Rodriguez[62], que distingue, dentro de los mismos, las siguientes fases: Toma de datos, Tratamiento de datos y Utilización y en su caso la comunicación de los mismos.

El tratamiento de los datos personales tiene un paso previo consistente en la recogida de datos y otro posterior en la utilización de los resultados obtenidos como consecuencia de ese tratamiento. La definición de estas fases debe servir como esquema previo para el análisis de tratamientos complejos, y nos permitirá sistematizar el estudio de la materia así como identificar los riesgos y obligaciones asociados a cada uno de ellos.

62 DAVARA RODRIGUEZ, M.A. (2006) *Manual de Derecho Informático*. Editorial Thompson Aranzadi. Madrid. Página 69.

3. Dato de carácter personal

3.1. El Dato

La LOPD contiene un definición de "dato" muy amplia, que hace referencia a "*cualquier información*", sin que quepa establecer limitaciones en función de la materia o de la mayor o menor relación o proximidad que el mismo tenga con el ámbito de la intimidad de la persona.

Tal y como establece Messia de la Cerda[63], el legislador no trata de de proteger un tipo de dato referente a personas en concreto, en todo caso, los supuestos de sensibilidad especial respecto al ámbito de la intimidad del interesado, son reconocidos por la LOPD en forma de una protección reforzada. Por el contrario, se pretende evitar los efectos que podría tener el tratamiento de un conjunto de datos personales, muchos de ellos insustanciales, pero susceptibles de ofrecer información relevante en función del tratamiento que de ellos se realice.

Por este motivo el legislador evita elaborar un *numerus clausus* de supuestos en los que considera que nos encontraremos ante un dato personal y realiza una descripción lo suficientemente amplia como para acoger los distintos tipos de datos que en función de su conexión con una persona física pueden considerarse datos de carácter personal. Por lo tanto, no se establecen límites al concepto de dato personal en función de su forma, manifestación o soporte.

Este criterio se refleja más claramente en la definición de dato de carácter personal contenida en el Reglamento de desarrollo de la LOPD:

«Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables».

El Reglamento enumera expresamente distintas formas que pueden ser adoptadas por los datos personales pero reconoce expresamente la posibilidad de que el dato personal pueda presentarse en "cualquier otro tipo" de formato.

63 MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto (2000). *La cesión o comunicación de datos de carácter personal*. Editorial Thompson Civitas. Agencia de Protección de Datos de la Comunidad de Madrid. Madrid.

3.2. La conexión a una persona identificada o identificable

Punto clave que deberemos considerar a la hora de calificar un dato como dato de carácter personal: La conexión de este dato con una persona física identificada o identificable.

Los datos deben identificar al sujeto o al menos deben hacer esta identificación factible. La identificación no se limita a las acciones tendentes a conocer la identidad de una persona, sino que se extiende a la posibilidad de poder elaborar perfiles más o menos detallados sobre dichas personas. Así, el artículo 2 a) de la Directiva 95/46 establece que la identificabilidad de los individuos afecta a su "*identidad física, fisiológica, psíquica, económica, cultural o social*".

En el mismo sentido, el artículo 5.1 Reglamento de desarrollo de la LOPD define "*persona identificable*" como:

«Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social».

Definición que además el reglamento completa de la siguiente forma:

«Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados»

A pesar de ser una definición extremadamente simple, la práctica nos pone en ocasiones en situaciones en las que puede resultar difícil determinar si nos encontramos o no ante un dato personal provocando problemas de interpretación, lo cual ha motivado que la Agencia Española de Protección de Datos así como los órganos de justicia se pronunciaran acerca de este extremo.

En este sentido podemos citar una consulta ante la Agencia sobre la naturaleza como datos personales de las matrículas de vehículos[64]:

«Para interpretar cuándo ha de considerarse que nos encontramos ante un dato de carácter personal esta Agencia ha venido siguiendo el criterio sustentado por las distintas Recomendaciones

64 Agencia Española de Protección de Datos (2006). Informe 425/2006: *Matrículas de vehículos y concepto de dato de carácter personal* [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0425_Matr-ii-culas-de-veh-ii-culos-y-concepto-de-dato-de-car-aa-cter-personal.pdf [2011, 7 de junio]

emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá considerarse identificable cuando su identificación no requiere plazos o actividades desproporcionados.

En este sentido se pronuncia el artículo 5 o) del Proyecto de Reglamento de desarrollo de la Ley Orgánica 15/1999, que fue sometido a informe de esta Agencia, habiendo el mismo sido emitido en fecha 17 de enero de 2007.

En consecuencia, el tratamiento de los datos correspondientes a las placas de matrícula de los vehículos se encontrará sometido a lo dispuesto en la Ley Orgánica 15/1999 en caso de que se considere a los datos contenidos en dichas placas datos de carácter personal, para lo que sería preciso que dichos datos pudieran permitir la identificación de un individuo sin que ello exija plazos o esfuerzos desproporcionados.

El artículo 5 h) del Texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto Legislativo 339/1990, de 2 de marzo, establece que "se atribuyen al Ministerio del Interior las siguientes competencias en el ámbito de esta Ley, sin perjuicio de las que tengan asumidas las Comunidades Autónomas en sus propios Estatutos (...) los registros de vehículos, de conductores e infractores, de profesionales de la enseñanza de la conducción, de centros de formación de conductores, de los centros de reconocimiento para conductores de vehículos a motor y de manipulación de placas de matrícula, en la forma que reglamentariamente se determine".

En consecuencia, el citado precepto reconoce la subsistencia del Registro de Vehículos, creado por el artículo 244 del Código de la Circulación, aprobado por Decreto de 25 de septiembre de 1934, habilitando expresamente al desarrollo reglamentario del Texto Refundido para establecer el régimen del citado Registro.

Dicho desarrollo se produjo a través de la aprobación del Reglamento General de Vehículos, en virtud de Real Decreto 2822/1998, de 23 de diciembre, cuyo artículo segundo establece en su párrafo primero que "la Jefatura Central de Tráfico llevará un Registro de todos los vehículos matriculados, que adoptará para su funcionamiento medios informáticos y en el que figurarán, al menos, los datos que deben ser consignados obligatoriamente en el permiso o licencia de circulación, así como cuantas vicisitudes sufran posteriormente aquéllos o su titularidad".

En cuanto a su finalidad, el párrafo segundo del precepto previene que "estará encaminado preferentemente a la identificación del titular del vehículo, al conocimiento de las características técnicas del mismo y de su aptitud para circular, a la comprobación de las inspecciones realizadas, de tener concertado el seguro obligatorio de automóviles y del cumplimiento de otras obligaciones legales, a la constatación del Parque de Vehículos y su distribución, y a otros fines estadísticos".

Por último, y en lo atinente a la publicidad de sus datos, el párrafo tercero del citado artículo 2 añade que "el Registro de Vehículos ... será público para los interesados y terceros que tengan interés legítimo y directo, mediante simples notas informativas o certificaciones". En consecuencia, se establece el carácter público del Registro, bastando para la consulta de sus datos la alegación de la existencia de un interés legítimo y directo en la consulta.

De lo que se ha venido indicando cabe desprender que la identificación del titular de los vehículos cuya matrícula sea conocida únicamente exigirá la consulta del Registro de Vehículos, cuya finalidad esencial es la identificación del titular, para lo cual únicamente será necesaria la invocación del interés legítimo del solicitante.

En consecuencia, cabe considerar que la identificación del titular del vehículo no exige esfuerzos o plazos desproporcionados, por lo que el tratamiento del dato de la matrícula habrá de ser considerado como tratamiento de un dato de carácter personal».

4. Fichero

4.1. El concepto de fichero en la LOPD

El artículo 3 de la LOPD establece el concepto de *fichero:*

«Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso»

Uno de los puntos más importantes para poder comprender la definición del concepto de fichero es la existencia de un **conjunto organizado** en los datos personales en él incluidos. Debemos tener en cuenta que sobre este concepto gira gran parte de las obligaciones impuestas por la normativa en materia de protección de datos de carácter personal. En este sentido es interesante destacar el artículo 43 LOPD:

*«**Responsables.***
1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.»

Debemos observar hasta que punto es importante este concepto que se impone como un requisito previo para la determinación de la existencia de responsabilidad la existencia, de forma previa, de un fichero con datos de carácter personal.

Sin embargo no debemos caer en el error de pensar que si no existen ficheros en una entidad la LOPD no se aplica. Al contrario, la Ley Orgánica de Protección de Datos aplica no sólo cuando existe un conjunto organizado de datos personales, sino también cuando se realiza cualquier tipo de operaciones y procedimientos que permitan la recogida, grabación, conservación, elaboración, bloqueo y cancelación de aquellos, aunque el responsable de ese tratamiento carezca de bases de datos de su titularidad tal y como establece la propia definición de fichero. Por tanto, las garantías de la LOPD son también aplicables a los responsables del tratamiento, aunque estos carezcan de ficheros de datos personales.

Además debemos tener en cuenta, en relación a la definición de fichero, que esta no especifica nada respecto al soporte o modo de gestión de los datos sino que, por el contrario, admite cualquier forma y que por lo tanto, las normas contenidas en la LOPD no solo resultan de aplicación a los datos almacenados en soporte automatizado, sino que también se aplicarán a aquellos que se encuentran almacenados en soporte papel. Es más, el Reglamento de desarrollo de la LOPD incluye en su articulado una definición de fichero no automatizado en su artículo 5.1. n):

«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».

4.2. Ficheros físicos y ficheros lógicos jurídicos

La amplitud de la definición de fichero ha generado una notable confusión en los responsables de aplicar la normativa en las organizaciones, ya que se ha otorgado la consideración de ficheros a conceptos informáticos como base de datos, aplicación, documento, etc. Esto ha llevado a declarar ante el Registro General de Protección de Datos un número altísimo de ficheros. Dichas prácticas se basan en una interpretación errónea de este concepto que dificulta enormemente la gestión del cumplimiento de las obligaciones de las organizaciones.

Por tanto, se hace necesario establecer con exactitud los conceptos de fichero físico así como de fichero lógico.

4.2.1 Fichero físico

Un fichero es un conjunto organizado de informaciones almacenadas en un soporte común. A dicha definición será necesario añadirle el calificativo de físico y, por tanto, ser conscientes que éstos pueden encontrarse en múltiples soportes: Ficheros en papel, aquellos contenidos en una determinada aplicación informática, aquellos conformados por un conjunto de archivos informáticos etc.

Por tanto, en una organización es habitual encontrar decenas o centenares de ficheros físicos que contienen datos personales ya que éstos se encuentran en aplicaciones y archivos informáticos que

contienen datos personales y que suelen generar a su vez una gran cantidad de pequeños ficheros creados por los responsables de cada área para variadas finalidades.

4.2.2. Fichero lógico

Un fichero lógico es un fichero o conjunto de ficheros físicos, que contienen el mismo tipo de datos, y que son tratados para una misma finalidad o finalidades compatibles. Es por tanto, a este concepto, el de fichero lógico al que debemos atenernos como objeto de las obligaciones que la LOPD impone.

En este sentido, las claves para llevar a cabo correctamente la identificación de los ficheros lógicos y la agrupación de los ficheros físicos en estas categorías pueden resumirse en dos:

- **Finalidad.** Los ficheros lógicos se identifican en función de la finalidad. Para cada finalidad señalaremos la existencia de un fichero lógico y será necesario cumplir con las exigencias de la LOPD.
- **Nivel de seguridad.** El objetivo de la agrupación de ficheros físicos en ficheros lógicos es registrar un solo fichero y aplicarle unas medidas de seguridad homogéneas[65]. Por ello, es conveniente que a los ficheros físicos agrupados en un fichero lógico les sea aplicable un mismo nivel de seguridad de acuerdo con lo establecido por el Reglamento de desarrollo de la LOPD.

Una vez realizada la agrupación, la identificación de los tratamientos de la información debe completarse de la siguiente manera:

- Determinación de las aplicaciones y sistemas que tratan los ficheros: ubicación física, responsables, etc.
- Determinación de los encargos del tratamiento así como de las cesiones.

65 En todo caso, las medidas de seguridad a aplicar a un fichero lógico serán las aplicables al fichero físico que tenga el nivel más alto.

4.3. Ficheros públicos y privados

La LOPD clasifica los ficheros distinguiendo entre públicos y privados. En este sentido, el Reglamento de desarrollo de la LOPD ha desarrollado las obligaciones ya recogidas en la LOPD para cada uno de estos tipos de ficheros e incluso ha aportado una mayor claridad a los conceptos, incluyendo las siguientes definiciones en los apartados l) y m) del artículo 5.1:

«***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*».

«***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*».

Como podemos observar, la distinción se aplica por lo tanto en función de la naturaleza pública o privada del responsable del fichero, regulándose la creación y mantenimiento de ambos tipos de ficheros en los capítulos I y II del Título IV de la LOPD.

Sin embargo esta clasificación no queda libre de dudas en relación a la aplicación de las obligaciones ya que la LOPD establece dos regímenes distintos. Esta situación fue resuelta por la Agencia a través de uno de sus múltiples informes[66] y que traemos en este punto a colación:

«Se consultó por una Entidad Pública Empresarial dependiente de una Comunidad Autónoma sobre el carácter público o privado de los ficheros de datos de que era responsable, lo que dio pie a considerar con carácter general la naturaleza pública o privada de los ficheros a la vista de lo establecido en la LOPD.

66 Agencia Española de Protección de Datos (2004). Informe 0000/2001: *Distinción entre ficheros de titularidad pública y privada* [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/naturaleza_pub_pri_ficheros/common/pdfs/2001-0000_Distinci-oo-n-entre-ficheros-de-titularidad-p-uu-blica-y-privada.pdf [2010, 7 de junio]

Como punto de partida, debe indicarse que la Ley no delimita de forma expresa los criterios delimitadores de la titularidad pública o privada de los distintos ficheros, si bien en el articulado del Capítulo I del Título IV viene a identificar los ficheros de titularidad pública como aquéllos cuya responsabilidad corresponde a las Administraciones Públicas (artículos 20 y 21), estableciendo ciertas especialidades en su régimen jurídico en las restantes disposiciones de este capítulo y en el artículo 46, en lo que se refiere al régimen sancionador. A partir de estos preceptos, deberá determinarse cuál es la interpretación que deba darse al término "titularidad pública", contenido en las citadas disposiciones, planteándose dos posibles criterios: por un lado el meramente subjetivo, que atiende a la naturaleza pública o privada del responsable del fichero; por otro, el criterio planteado por la consulta que atiende a la función desempeñada por dicho responsable.

Pues bien, como punto de partida, entendemos que, tal y como se desprende de las disposiciones de la LOPD, el criterio que ha de prevalecer en este punto es el relativo a la naturaleza pública o privada del responsable, ya que la Ley no se diferencia ambas categorías de ficheros con base en criterios relacionados con la actividad llevada a cabo por el responsable, sino con el criterio de la "titularidad" del fichero.

Así se desprende, no sólo de las rúbricas de los Capítulos I y II del Título IV de la Ley, sino de lo dispuesto en el artículo 46, que establece una especialidad en materia sancionadora para los supuestos de ficheros de titularidad pública, refiriéndose a los mismos como "ficheros de los que sean responsables las Administraciones Públicas", añadiendo, en su apartado segundo la posible imposición de las sanciones "establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas".

En el caso examinado, como se ha indicado, el responsable del fichero era una Empresa Pública, configurada por la norma legal que la creó como Entidad de derecho público sometida a lo dispuesto en esa la presente Ley y en sus disposiciones complementarias de desarrollo. Por lo que respecta a las relaciones jurídicas externas, a las adquisiciones patrimoniales y a la contratación, se establecía por ley su sujeción, sin excepciones, al derecho privado. También se indicaba en dicha norma legal que de los acuerdos que dictasen los órganos de gobierno de dicha Empresa Pública conocería la jurisdicción que en cada caso corresponda, sin necesidad de formular la reclamación previa en vía gubernativa.

De este último inciso se desprendía que la Entidad se encontraba incluso desprovista de las prerrogativas derivadas del procedimiento de reclamación previa al ejercicio de acciones civiles o laborales, reconocida por los artículos 120 y siguientes de la Ley 30/1992.

Por ello, no ostentando la responsable del fichero la condición de administración pública, sometida al derecho administrativo, resulta imposible considerar el fichero al que se refiere la consulta como de titularidad pública, siendo un fichero de titularidad privada, sometido a las disposiciones previstas en la LOPD para este tipo de ficheros.

Por otra parte, y en cuanto al criterio para discernir la naturaleza de la actividad desarrollada por la Entidad Pública que formuló la consulta, la cuestión preponderante implicaba atender al ejercicio, en su caso, por la misma, de auténticas potestades administrativas, en el término tradicional del término (tributaria, sancionadora, expropiatoria y disciplinaria); esto es, si la responsable del fichero se encontraba, en el ejercicio de las actividades relacionadas con el fichero, investido de imperium, lo que no sucedía en ese caso.

Todo ello aboca a la conclusión ya sostenida, consistente en considerar que el fichero al que se refiere la presente consulta es un fichero de titularidad privada, quedando sometido a las disposiciones contenidas en el Capítulo II del Título IV de la Ley Orgánica 15/1999».

4.3.1. Creación, modificación y supresión de ficheros de titularidad pública

Para los ficheros de **titularidad pública**, es el artículo 20 LOPD el que regula los medios para su creación, modificación o supresión, estableciendo las siguientes condiciones:

- La creación, modificación o supresión de los ficheros públicos sólo podrá hacerse por medio de disposición general publicada en el *Boletín Oficial del Estado* o Diario oficial correspondiente.
- Estas disposiciones de creación o de modificación de ficheros deberán indicar:
  - La finalidad del fichero y los usos previstos para el mismo.
  - Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
  - El procedimiento de recogida de los datos de carácter personal.

- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- Los órganos de las Administraciones responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

- En caso de la supresión de los ficheros, la disposición establecerá el destino de los ficheros o, en su caso, las previsiones que se adopten para su destrucción.

El Reglamento de desarrollo de la LOPD completa el régimen jurídico de aplicación a los ficheros de titularidad pública, regulando aspectos como los supuestos de inscripción de oficio de estos ficheros. De acuerdo con el artículo 63 Reglamento de desarrollo de la LOPD, en supuestos excepcionales, y con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la subsistencia de la obligación de notificación, se podrán inscribir de oficio por el Director de la Agencia Española de Protección de Datos, y a propuesta del Registro, ficheros de titularidad pública.

4.3.2. Creación, modificación y supresión de ficheros de titularidad privada

A. Creación

Queda establecido en el **artículo 25 de la LOPD:**

«Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o Entidad titular y se respeten las garantías que esta ley establece para la protección de las personas»

Las condiciones para crear un fichero de titularidad privada son las siguientes:

- **La notificación debe ser previa a la creación**.
- Los ficheros deben notificarse a la Agencia Española de Protección de Datos por la persona o Entidad que pretenda crearlos siendo necesario indicar:

- Identificación del responsable del fichero.
- Identificación del fichero.
- Finalidades y usos previstos.
- El sistema de tratamiento empleado en su organización.
- El colectivo de personas sobre el que se obtienen los datos.
- El procedimiento y procedencia de los datos.
- Las categorías de datos.
- El servicio o unidad de acceso.
- La indicación del nivel de medidas de seguridad básico, medio o alto.
- En su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

En lo relativo al responsable del fichero, el artículo 57 del Reglamento de desarrollo de la LOPD prevé que en el caso de que exista más de un responsable, cada una de ellos deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto.

B. Modificación y supresión

El artículo 58 del Reglamento de desarrollo de la LOPD regula el supuesto de modificación y supresión de ficheros, y resulta de aplicación tanto a ficheros de titularidad pública como de titularidad privada. El Reglamento exige a este respecto:

- La inscripción del fichero deberá encontrarse actualizada en todo momento.
- Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos.
- Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

4.4. Limitación al ámbito objetivo de aplicación de la LOPD

4.4.1. Ficheros que constituyen excepciones concretas a la LOPD

El artículo 2.2 de la LOPD establece:

«2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
a. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos"

Como podemos observar nos encontramos en presencia de límites al ámbito objetivo de aplicación de la LOPD. En este sentido, el primero de ellos alude a una limitación imprescindible que afecta al ámbito privado de las personas y en los otros dos casos, la LOPD hace referencia a materias que por su importancia para la seguridad justifican la excepción en la aplicación de la LOPD cuyos criterios serían incompatibles con las finalidades de estos tratamientos.

A. Ficheros mantenidos por personas físicas en actividades personales

Una limitación evidente ya que en caso contrario, todos los particulares estarían obligadas a cumplir con los requisitos establecidos por la LOPD. El Reglamento de desarrollo de la LOPD ha venido a completar la regulación de la LOPD en este punto, definiendo que debe entenderse por *"actividades personales o domésticas"* y poniéndolo en relación con los conceptos de *"vida privada o familiar"*. Tal y como establece el artículo 4 a) del Reglamento de desarrollo de la LOPD:

«Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los

particulares».

B. Ficheros sometidos a normativa sobre materias clasificadas

En virtud de la Ley 9/1968, de 5 de abril, de Secretos Oficiales, modificada por la Ley 48/1978, de 7 de octubre, podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puede dañar o poner en riesgo la seguridad y defensa del Estado, no siéndoles de aplicación la LOPD.

C. Ficheros creados para la investigación del terrorismo y formas graves de delincuencia organizada

En este caso si será necesario que la Agencia Española de Protección de Datos tenga conocimiento de la creación de este tipo de ficheros tal y como establece expresamente el artículo 4 c) del Reglamento de desarrollo de la LOPD.

4.4.2. Ficheros regulados por disposiciones específicas

Nos encontramos en presencia de ficheros que tratan datos referidos a materias que, por su importancia, son reguladas por otras disposiciones. Según el artículo 2.3 de la LOPD:

«3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:
a. Los ficheros regulados por la legislación de régimen electoral.
b. Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c. Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d. Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e. *Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia"*

A. Normativa de Régimen Electoral

Los datos personales gestionados en el marco del régimen electoral, se regirán por las siguientes normas:

- Ley Orgánica 5/1985, de 19 de junio sobre Régimen Electoral General así como por las modificaciones realizadas a ésta.
- Ley 7/1987, de 2 de abril, sobre Bases de Régimen Local. Esta norma establece que uno de los objetivos que el legislador persigue en este ámbito es procurar que los padrones puedan permitir a los Ayuntamientos remitir, debidamente actualizados, los datos requeridos para el mantenimiento del censo electoral.

B. Ficheros afectados por la legislación sobre la función estadística pública

Datos que solo sirven a fines estadísticos de acuerdo a lo previsto por la Ley 12/1989 de 9 de mayo de la Función Estadística Pública o la legislación autonómica específica. No obstante, pese a que los ficheros con fines estadísticos están regulados por esta normativa, el artículo 37.1 m) de la LOPD establece algunos ámbitos de competencia de la Agencia Española de Protección de Datos en la materia:

«Son funciones de la Agencia Española de Protección de Datos: (…)
m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46»

C. Ficheros afectados por la legislación del régimen del personal de las fuerzas armadas

Los tratamientos de datos personales que se lleven a cabo respecto al personal de las Fuerzas Armadas son regulados por la Ley 17/1999, de 18 de mayo, que establece la creación de un registro de todos los militares profesionales que estará ubicado y gestionado por el Ministerio de Defensa.

D. Tratamientos derivados del registro civil y del registro central de penados y rebeldes

Serán de aplicación:

- Real Decreto 1138/1969, de 22 de mayo, modificado por el Real Decreto 1917/1986, de 29 de agosto, que regula los requisitos de publicidad del Registro Civil, así como las limitaciones de acceso a datos y al régimen de cancelaciones y rectificaciones.
- Ley Orgánica 7/1992, de 27 de noviembre, que se refiere al Registro Civil desde el punto de vista de su informatización.
- Ley orgánica 1/1979, de 26 de septiembre, General Penitenciaria.
- Real Decreto 190/1996, de 9 de febrero, en el que se trata la protección de los datos de carácter personal de los ficheros penitenciarios.

E. Ficheros de grabaciones efectuadas por las Fuerzas y Cuerpos de Seguridad

La norma de aplicación en este ámbito será la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares Públicos así como su norma de desarrollo, el Real Decreto 596/1999, de 16 de abril.

4.5 Ficheros privados con Régimen Especial

En este punto vamos a hacer una referencia a dos tipos de ficheros que la LOPD y el Reglamento de desarrollo de la LOPD regulan expresamente: los ficheros de solvencia patrimonial y crédito y los ficheros de publicidad y prospección comercial. Son dos supuestos en los que el legislador prevé variaciones sobre el régimen general de principios y derechos y que la LOPD reconoce respecto al resto de los tratamientos de datos personales.

4.5.1. Ficheros de solvencia patrimonial y crédito

Se encuentran regulados en el artículo 29 de la LOPD:

*«**Artículo 29**. Prestación de servicios de información sobre solvencia patrimonial y crédito.*
1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.
3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o Entidad a quien se hayan revelado los datos.
4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos»

En palabras de Almuzara Almaida[67] estos ficheros, contribuyen a la salvaguarda del sistema financiero al permitir a las entidades financieras conocer la solvencia de sus clientes o potenciales, quienes de estos han incurrido en morosidad, porque cuantía y proporcionar igual conocimiento a empresas, (sobre todo PYMES) a la que una situación de incumplimiento de sus clientes pudiera ocasionarles un grave quebranto.

Si bien este tipo de tratamientos tienen una utilidad cierta, no es menos evidente que la inclusión de sus datos personales en los mismos tendrá consecuencias graves para el titular de los mismos. Por este motivo la LOPD impone una serie de limitaciones a estos tratamientos. En el mismo sentido, la Agencia estableció en su Instrucción de 1/1995 una interpretación de las disposiciones propias para este tipo de ficheros.

En la actualidad, el régimen jurídico de aplicación a estos tratamientos se completa a través del Capítulo I del Título IV del Reglamento de desarrollo de la LOPD (artículos 37 a 44). Si analizamos con detalle la regulación de este tipo de ficheros y, tal y como afirma Isabel Herrán Ortiz[68], la verdadera excepcionalidad en la regulación de estos ficheros de datos personales, radica en la admisibilidad de obtener del acreedor datos con estos fines, ello sin que expresamente se establezca la exigencia del consentimiento del afectado, por lo que la información se registrará válidamente a efectos del cumplimiento o no de las obligaciones dinerarias sin que el interesado haya prestado su consentimiento al respecto.

Por tanto, adquiere especial significación el derecho de información en el supuesto de que la información se haya facilitado por el acreedor o por persona que actúe por su cuenta, ya que posteriormente sí será preciso ofrecer dicha información, en los términos y plazo establecidos por la normativa. A la vista de esta excepcionalidad, la Instrucción 1/1995[69] ya estableció una serie de motivos tasados para la inclusión de los datos en este tipo de ficheros.

Por su parte, el Reglamento de desarrollo de la LOPD ha venido a recoger estos motivos en su artículo 38 que establece que sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, si concurren

67 ALMUZARA ALMAIDA, Cristina (2005). *Ficheros privados con régimen especial. Parte I: Solvencia Patrimonial y Crédito, Estudio práctico sobre la protección de datos personales*. Lex Nova. Valladolid.

68 HERRAN ORTIZ, Isabel (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Dyckson, Madrid.

69 Agencia Española de Protección de Datos (1995). «*Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.*» [en línea]. Disponible en: http://www.agendaactiva.es/default.aspx?info=0000E7 [2010, 10 de junio]

los siguientes requisitos:

- Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.
- Que no hayan transcurrido **seis años** desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.
- Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.
- No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.

Dentro de este tipo de ficheros podemos distinguir entre:

- **Ficheros de solvencia.** Recogen información sobre solvencia patrimonial y de crédito de carácter positivo, es decir, hacen referencia a las posibilidades económicas de los titulares de los datos recogidos.
- **Ficheros de cumplimiento e incumplimiento de obligaciones dinerarias.** Creados con la finalidad del almacenamiento de datos relativos al cumplimiento de obligaciones dinerarias.

4.5.2 Ficheros de publicidad y prospección comercial

Regulados en el artículo 30 LOPD:

«***Artículo 30. Tratamientos con fines de publicidad y de prospección comercial***

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

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.
3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.
4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud».

En este sentido, la LOPD reconoce dos fuentes para la obtención de información:

- El propio interesado.
- Fuentes de acceso público. En este caso en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asistan.

5. Tratamiento de datos de carácter personal

5.1 Los tratamientos de datos de carácter personal

Tal y como establece el artículo 5 del Reglamento de desarrollo de la LOPD, un tratamiento de datos es:

«Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

En base a la presente definición podemos extraer las siguientes conclusiones:

- Se considerará “tratamiento” cualquier operación que llevemos a cabo sobre datos personales.

- Y se considerará tratamiento, con independencia de que éste **"sea o no automatizado**".
- La definición de tratamiento de datos personales debe ponerse en relación con la de fichero. Para que la LOPD sea aplicable a un tratamiento, este deberá encontrarse contenido en un fichero.

En este punto y como medio de examen de la naturaleza de los tratamientos sometidos a la LOPD y su Reglamento de desarrollo conviene citar la Sentencia de la Audiencia Nacional de fecha 16 de febrero de 2006[70] en la que el tribunal hace referencia al tratamiento, siguiendo el siguiente análisis:

«Para abordar el concepto de "tratamiento de datos personales" y el de "fichero" desde la perspectiva legal hemos de partir de la Directiva 95/46,/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, Directiva de la que nuestra actual leyes tributaria en gran medida.

Esta Directiva nos dice, en primer lugar, que ***el concepto de "tratamiento" no puede depender de la técnica utilizada para el maneja de los datos****, de ahí que incluya tanto el tratamiento automatizado como el manual (considerando 27 de su Preámbulo). Así,* ***lo relevante para que estemos ante un "tratamiento de datos personales" es la realización de determinadas actuaciones en relación con los mismos, actuaciones que en su descripción son muy amplias y variadas.***

Desarrollando este principio, el artículo 2 de la Directiva describe las actuaciones que aplicadas a los datos personales constituyen "tratamiento": "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".

Nuestra ley lo define de forma muy similar en el arto 3.c) de la Ley Orgánica 15/1999.

"c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas,

70 Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 16 de Febrero 2006. Recurso 511/2004

interconexiones y transferencias."

No basta, sin embargo, la realización de una de estas actuaciones en relación con datos personales para que la ley despliegue sus efectos protectores y sus garantías y derechos del afectado. Es preciso algo más: que las actuaciones de recogida, grabación, conservación etc... se realicen de forma automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a un fichero»

5.2 Tratamientos sujetos a aplicación legal

El artículo 2.1 de la LOPD establece su ámbito geográfico de aplicación:

*«**Artículo 2.** Ámbito de aplicación. (…) .*
Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
a. Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b. Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c. *Cuando el responsable del tratamiento no este establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito».*

Esta cuestión no es baladí puesto que en la actualidad es posible, con independencia del lugar en el que se ubique el fichero, tratar la información en él contenida desde distintos puntos geográficos. Por esta razón, ya la Directiva 95/46/Ce establece la sujeción a la legislación nacional de estas actividades cuando las mismas se estén desarrollando en el territorio del citado país, y ello con independencia del lugar donde esté establecido el responsable del tratamiento de datos, ya que en ningún caso dicha circunstancia deberá poder obstaculizar o afectar al grado de protección de las personas en el tratamiento de sus datos personales[71].

Debe tenerse en cuenta que la ubicación de los medios y el ejercicio de la actividad o tratamiento determinará que sea la legislación española de protección de datos la aplicable a dicho tratamiento, sin que pueda argumentarse en contra que el establecimiento del responsable del tratamiento se

71 Considerandos 21 y 22 de la Directiva 95/46/CE.

halla fuera de nuestro país. Por tanto, se hace imprescindible proteger al titular de los datos en todas las situaciones que estas posibilidades implican. Por esta razón el artículo 2.1 de la LOPD establece las bases enunciadas con anterioridad.

En este punto conviene citar la resolución a una consulta planteada a la Agencia Española de Protección de Datos[72] sobre si procede la notificación al registro General de Protección de Datos de los tratamientos llevados a cabo por la consultante en el marco de una actividad desarrollada en otro país miembro de la UE y según la cual se reciben solicitudes de compra formuladas en un portal de compra on-line ubicado en España:

*«En consecuencia**, la legislación española sería aplicable a los tratamientos llevados a cabo en el marco de las actividades de un responsable del tratamiento situado en territorio español**, razón por la cual el tratamiento desarrollado por la consultante, llevado a cabo por una Entidad ubicada en Irlanda, no se encontraría sometido a la ley española, no siendo en consecuencia precisa su inscripción en el Registro General de Protección de Datos de esta Agencia»*

También podemos citar una consulta[73] sobre si resulta de aplicación la LOPD a los tratamientos llevados a cabo a bordo de un buque de nacionalidad no española que atraviesa aguas españolas:

«(…) En definitiva, el supuesto planteado se encontraría sometido a la Ley española en caso de que pudiera considerarse el buque al que la consulta se refiere un establecimiento del responsable del fichero ubicado en España o que se utilizasen en el tratamiento medios ubicados en territorio español.

A nuestro juicio, el hecho de que el buque atraviese aguas españolas no implica que los medios empleados para el tratamiento se encuentren ubicados en territorio español, habida cuenta que la expresión contenida en el artículo 4.1 c) de la Directiva debe considerarse aplicable a aquellos medios ubicados en dicho territorio de una forma permanente, como por ejemplo, si en la transmisión de los datos fuera empleada una red pública de comunicaciones electrónicas ubicada

72 Agencia Española de Protección de Datos (2005). Informe 0026/2005: *Transmisión de datos dentro de la Unión Europea* [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2005-0026_Transmisi-oo-n-de-datos-dentro-de-la-Uni-oo-n-Europea.pdf [2010, 10 de junio]

73 Agencia Española de Protección de Datos (2005). Informe 0334/2005: *Tratamiento de datos realizados a bordo de buques* [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2005-0334_Tratamiento-de-datos-realizados-a-bordo-de-buques.pdf [2010, 10 de junio]

en España, pero no a aquellos casos en los que la ubicación de los medios del tratamiento sea meramente accidental o contingente, dado que en ese caso, resultará obvio que esa contingencia implicará que el medio sea, en el peor de los supuestos "de mero tránsito".

(…) De todo ello se desprende que, salvo que los datos objeto de tratamiento a bordo del buque sean transmitidos a un fichero ubicado en España, no será necesario en relación con dichos tratamientos el cumplimiento de las obligaciones previstas en la legislación española en materia de protección de datos, toda vez que el tratamiento no se encontrará sometido a la misma»

5.3 Fases

Tal y como establece Davara Rodriguez[74], en un tratamiento de datos personales podemos distinguir las siguientes fases: Toma de datos, tratamiento de datos, utilización y en su caso comunicación.

5.3.1 Toma de datos.

La toma de datos se realizará sobre soportes de obtención de datos personales, ya sean automatizados o no. Uno de los primeros aspectos que debemos analizar en el momento de la identificación de un tratamiento de información con relevancia desde el punto de vista del derecho a la protección de datos personales, son los puntos de recogida de datos.

En el momento de la recogida, la Ley establece una serie de obligaciones para garantizar los derechos de los titulares de datos y la identificación de estos puntos de recogida, resulta esencial para garantizar el cumplimiento de estas obligaciones.

5.3.2 Tratamiento de datos.

Recoge todos las operaciones que el responsable del fichero lleva a cabo sobre los datos. La LOPD considerará tratamiento a prácticamente cualquier actividad: grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión. Por tanto, toda

74 DAVARA RODRIGUEZ, Miguel Ángel (2006). *Manual de Derecho Informático*. Editorial Thompson Aranzadi. Madrid. Página 69.

operación sobre los datos de carácter personal debe estar sometida a lo establecido en la LOPD.

5.3.3 Utilización y en su caso, comunicación de los datos.

El tratamiento se realiza con la intención de llevar a cabo una utilización de los datos para obtener, información a partir de los datos y, eventualmente, para ceder dichos datos, o dicha información a terceros en distintos marcos de cesión y que pueden corresponder a esquemas de comunicación de datos o de encargos del tratamiento.

6. Ámbito subjetivo

6.1 Empresarios individuales

Nos encontramos en presencia de uno de los supuestos más controvertidos de cara a su aplicación y para cuyo análisis nos centraremos en el estudio realizado por la Agencia Española de Protección de Datos en el Informe 42/2008[75].

6.1.1 Aplicación de la LOPD

El artículo 2.1 de la LOPD establece:

«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».

Mientras que gracias al artículo 3 de la LOPD conocemos que "dato personal" es cualquier información concerniente a personas físicas identificadas o identificables. De estos preceptos se deduce que la protección conferida por la LOPD no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas por la citada norma, siempre sin perjuicio de que los Tribunales puedan atender las reclamaciones de responsabilidad que pudieran exigirse en el caso de que el uso de información relativa a las empresas les cause algún perjuicio. Por lo tanto, las previsiones de la LOPD no son de aplicación a los datos referidos a personas jurídicas. Sin embargo, ¿que sucede con los datos de empresarios individuales?.

Para ello deberemos basarnos en lo establecido por la Agencia Española de Protección de Datos, en su Resolución de 27 de febrero de 2001, en cuyo Fundamento Jurídico II establece:

«... la protección conferida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no es aplicable a las personas jurídicas, que no gozarán de ninguna

75 Agencia Española de Protección de Datos (2005). Informe 0042/2002 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0042_Novedades-del-Reglamento-respecto-a-empresarios-individuales..pdf [2010, 10 de junio]

de las garantías establecidas en la Ley, y por extensión lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando, en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y con los empresarios individuales que ejercen una actividad comercial y respecto de las cuales sea posible diferenciar su actividad mercantil de su propia actividad privada, estando en el primer caso excluidos también del ámbito de aplicación de la Ley Orgánica 15/1999.

En definitiva pues, tanto las personas jurídicas como los profesionales y los comerciantes individuales (éstos dos últimos sólo en los estrictos términos señalados en el párrafo que antecede, esto es, cuando sus datos hayan sido tratados tan sólo en su consideración de empresarios) quedan fuera del manto protector de la Ley Orgánica 15/1999.

A contrario sensu, tanto los profesionales como los comerciantes individuales quedarían bajo el ámbito de aplicación de la Ley Orgánica 15/1999 y, por tanto, amparados por ella cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando, en consecuencia, la condición de comerciante (es el caso de los profesionales liberales cuyas actividades están expresamente excluidas del ámbito de aplicación de la Ley Básica 3/1993 por su artículo 6) y los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada.

En estos dos casos deberán aplicarse siempre las garantías de la Ley Orgánica 15/1999 dada la naturaleza fundamental del derecho a proteger.

Ello exigirá siempre ir analizando caso por caso para hallar en cada supuesto concreto el límite fronterizo donde resulte afectado el derecho fundamental a la protección de datos de los interesados personas físicas, o, por el contrario, aquél no resulte amenazado por incidir tan solo en la esfera de la actividad comercial o empresarial, teniendo en todo caso presente que, en caso de duda, la solución deberá siempre adoptarse a favor de la protección de los derechos individuales».

En idéntico sentido, la Sentencia del Tribunal Supremo de 20 de febrero de 2007[76], refiriéndose específicamente a profesionales, se pronuncia sobre este tema en su fundamento de derecho sexto párrafo octavo donde señala que:

76 Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 6ª, Sentencia de 20 de febrero de 2007. Recurso 732/2003.

«Es claro que los Arquitectos y Promotores a que se refiere el litigio participan de la naturaleza de personas físicas y que no dejan de serlo por su condición de profesionales o agentes que intervienen en el mercado de la construcción, por lo que los datos personales relativos a los mismos, quedan amparados y sujetos en cuanto a su tratamiento informatizado a las previsiones de la LORTAD; y es que desde este punto de vista subjetivo la exclusión del ámbito de aplicación de la LORTAD no viene determinado por el carácter profesional o no del afectado o titular de los datos objeto de tratamiento, sino por la naturaleza de persona física o jurídica titular de los datos, en cuanto sólo las personas físicas se consideran titulares de los derechos a que se refiere el art. 18.4 de la Constitución».

Adicionalmente, el informe de la Agencia Española de Protección de Datos de 14 de febrero de 2006[77], referido al tratamiento de los datos de facturación de las oficinas de farmacia, hace referencia a los supuestos en los que se confundan persona física y titular del establecimiento, basando su análisis en la legislación mercantil y estableciendo que no será aplicable, a este dato, la LOPD:

«El problema podría plantearse en los supuestos en que en virtud de una libre decisión del titular de la oficina de farmacia haya decidido denominarse dicho establecimiento mercantil con sus propios datos identificativos, ya sea como consecuencia de una decisión de estrategia empresarial, no olvidemos la naturaleza de comerciante del titular de la oficina a la que nos hemos referido, ya sea en virtud de cualquier otra causa.

En ese supuesto, como consecuencia de la mencionada decisión, sería posible que al accederse a los datos de facturación de la oficina a partir de la denominación de la misma no se accediese a una mera denominación objetiva, sino a los datos de nombre y apellidos o a alguno de estos datos, del titular de la oficina, por lo que podría considerarse aplicable al caso el artículo 2.1 de la Ley Orgánica 15/1999, en conexión con la definición otorgada al mismo del concepto de datos de carácter personal, dado que el nombre y apellidos harían identificable al titular.

No obstante, el hecho de que el establecimiento mercantil se denominase con el nombre y apellidos del titular no convertiría dicho establecimiento en una persona física.

77 Agencia Española de Protección de Datos (2006). Informe 0119/2006: *Cesión de datos de facturación de las oficinas de farmacia* [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2006-0119_Cesi-oo-n-de-datos-de-facturaci-oo-n-de-las-oficinas-de-farmacia..pdf [2010, 10 de junio]

En este sentido, debe recordarse que la legislación mercantil impone en determinados supuestos la obligación de que la denominación social de una determinada persona jurídica se corresponda precisamente con los datos identificativos de los socios que la componen.

Así, el artículo 126 del Código de Comercio señala que "la Compañía colectiva deberá girar bajo el nombre de todos sus socios, de algunos de ellos o de uno solo, debiéndose añadir, en estos dos últimos casos, al nombre o nombres que se expresen las palabras «y Compañía»"

Igualmente, según el artículo 146 del propio Código "la compañía en comandita girará bajo el nombre de todos los socios colectivos, de algunos de ellos o de uno solo, debiendo añadirse, en estos dos últimos casos, al nombre o nombres que se expresen las palabras «y Compañía», y en todos, las de «sociedad en comandita»".

Por último, en relación con la denominada Sociedad Limitada de la Nueva Empresa, el artículo 131 de la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada, introducido por la Ley 7/2003, de 1 abril, dispone que "La denominación social estará formada por los dos apellidos y el nombre de uno de los socios fundadores seguidos deun código alfanumérico que permita la identificación de la sociedad de manera única e inequívoca"».

Por lo tanto, existen supuestos en los que los datos identificativos de una persona física puedan corresponderse con la denominación de una persona jurídica, el rótulo de un establecimiento mercantil o la marca de un determinado producto o servicio o de una gama de los mismos. Sin embargo, ello no alterará el hecho de que dichas denominaciones identificarán a la persona jurídica, al establecimiento o al producto o gama, sin que puedan ser considerados a efectos de lo dispuesto en la LOPD como datos de carácter personal.

6.1.2 Aplicación del Reglamento de desarrollo de la LOPD

El artículo 2.3 del Reglamento de desarrollo de la LOPD establece:

«Los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal».

Este artículo no hace sino afirmar la interpretación que ha venido realizando la Agencia Española de Protección de Datos respecto al texto de la LOPD.

Por tanto, no podrá considerarse amparado por el precepto, y en consecuencia excluido de la aplicación de la LOPD, el tratamiento de los datos del comerciante llevado a cabo no con la finalidad de mantener una relación empresarial con el establecimiento u organización que el mismo hubiera creado, sino para conocer la información del propio sujeto organizado en forma de empresa, siendo el destinatario del tratamiento no la empresa sino el propio empresario en tanto, por ejemplo, que consumidor individual. De esta forma podemos extraer las siguientes conclusiones:

- La legislación de protección de datos no es aplicable en los supuestos en los que los datos del comerciante sometidos a tratamiento hacen referencia únicamente al mismo en su condición de comerciante, industrial o naviero; es decir, a su actividad empresarial.
- El uso de los datos deberá quedar limitado a las actividades empresariales; es decir, el sujeto respecto del que pretende llevarse a cabo el tratamiento es la empresa constituida por el comerciante industrial o naviero y no el empresario mismo que la hubiese constituido. En caso de que la utilización de los datos se produjera en relación con un ámbito distinto quedaría plenamente sometida a las disposiciones de la LOPD.

Por su parte, el artículo 2.2 del Reglamento de desarrollo de la LOPD, incluye otra limitación al marco de aplicación haciendo referencia a los denominados "*ficheros de contactos en las empresas*":

«Este Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales».

Además, el Reglamento de desarrollo de la LOPD también ha venido a recoger la interpretación de la Agencia Española de Protección de Datos que en su Resolución de 19 de julio de 2005[78] se refiere a la grabación de una conversación telefónica en la que participan como interlocutores el denunciante, en su calidad de administrador único de una sociedad y el administrador de la empresa imputada, referida exclusivamente a la adquisición de una finca:

78 Agencia Española de Protección de Datos (2005). Resolución de 19 de julio de 2005.

«(...) ambos interlocutores intervienen en el presente supuesto, como ha quedado acreditado, en el desempeño de las funciones de apoderamiento que le son propias como representantes de las citadas entidades, desarrollando, en todo momento, una actividad mercantil claramente separada de sus respectivas actividades privadas.

(...) los hechos expuestos se circunscriben a unas actuaciones desarrolladas, por los representantes de las sociedades implicadas, exclusivamente en el ámbito de actuación de las mismas, y en concreto en el desarrollo de la actividad inmobiliaria que constituye su objeto social, que, como ha quedado señalado, comprende la construcción, promoción, adquisición y venta de inmuebles.

En consecuencia, el tratamiento de los datos de que traen causa las presentes actuaciones de inspección no se encuentra incluido dentro del ámbito de aplicación establecido en la LOPD».

Asimismo, las Resoluciones de 24 de agosto de 2005[79] y 9 de mayo de 2006[80] se refieren al tratamiento de direcciones de correo electrónico en que figuran algunos nombres de personas de la empresa con la que el responsable del tratamiento mantuvo relación comercial, considerando la segunda de las resoluciones citadas que *"se trata de direcciones institucionales de empresa que, por lo tanto, no tienen la consideración de dato personal, por lo que procede acordar el archivo de las presentes actuaciones previas de investigación"*.

En este sentido es importante resaltar que siempre será necesario que el tratamiento del dato de la persona de contacto sea accesorio en relación con la finalidad perseguida, requisito que puede dar lugar a distintas interpretaciones. Lo mejor por tanto, es cumplir siempre con dos aspectos concretos:

- Que los datos tratados se limiten efectivamente a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios y, en concreto[81]:
  - Nombre y apellidos
  - Funciones o puestos desempeñados

79 Agencia Española de Protección de Datos (2005). Resolución de 24 de agosto de 2005.
80 Agencia Española de Protección de Datos (2006). Resolución de 9 de mayo de 2006.
81 Cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la LOPD, por exceder de lo meramente imprescindible para identificar al sujeto en cuanto contacto de quien realiza el tratamiento con otra empresa o persona jurídica.

- Dirección postal o electrónica
- Teléfono y número de fax profesionales

- Que la inclusión de los datos de la persona de contacto sea meramente accidental o incidental respecto de la verdadera finalidad perseguida por el tratamiento, que ha de residenciarse no en el sujeto, sino en la Entidad en la que el mismo desarrolla su actividad o a la que aquél representa en sus relaciones con quienes tratan los datos.

Por esta razón, la finalidad del tratamiento debe perseguir una relación directa entre quienes traten el dato y la Entidad y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esa finalidad.

6.2 Tratamiento de datos de personas fallecidas

El artículo 32 del Código Civil establece que *«la personalidad civil se extingue por la muerte de las personas»*.

En principio, la muerte extingue los derechos inherentes a la personalidad. En el mismo sentido, la Agencia Española de Protección de Datos ha venido tradicionalmente poniendo de manifiesto que el derecho fundamental a la protección de datos es un derecho personalísimo que, en consecuencia, se extingue por la muerte de las personas. Para ello ha aducido la vinculación existente entre el derecho a la protección de datos y la intimidad de las personas, y esta consideración debe seguir considerándose vigente tras la configuración otorgada a la protección de datos como derecho fundamental de la persona por la Sentencia 292/2000, de 30 de noviembre del Tribunal Constitucional.

Si el derecho fundamental a la protección de datos ha de ser considerado como el derecho del individuo a decidir sobre la posibilidad de que un tercero pueda conocer y tratar la información que le es propia, es evidente que dicho derecho desaparece por la muerte de las personas, por lo que los tratamientos de datos de personas fallecidas no podrían considerarse comprendidos dentro del ámbito de aplicación de la normativa en materia de protección de datos de carácter personal.

Sin embargo, debemos tener en cuenta que si bien el derecho a la protección de datos desaparecería como consecuencia de la muerte de las personas, no sucede así con el derecho de determinadas personas de ejercitar acciones en nombre de las personas fallecidas con el fin de garantizar otros derechos constitucionalmente reconocidos.

En este sentido, la Ley Orgánica 1/1885, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pone de manifiesto en sus artículos 4 a 6 que el fallecimiento no impide que por las personas que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya designado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal, interpretación que ha sido recogida por el artículo 2.4 del Reglamento de desarrollo de la LOPD:

«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»

II. PRINCIPIOS

1. Introducción

Los denominados *"principios de protección de datos"*, tuvieron su primera expresión en el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El Convenio ha sido por lo tanto el punto de partida de la normativa posterior en esta que se ha desarrollado sobre un proceso conforme al cual[82]:

«Ha ido cristalizando la "opinio iuris" generada a lo largo de dos décadas y definiendo derechos y garantías encaminadas a asegurar la observancia de los principios generales de protección de datos recogidos en el mismo».

Y que ya podía observarse en la Exposición de Motivos de la LORTAD:

«Los principios generales definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de los datos almacenados cuanto la congruencia y la racionalidad de la utilización de datos»

En idéntico sentido, la Directiva 95/46/CE, nos muestra los principios de protección de datos, precisándolos y ampliándolos de acuerdo con lo declarado en sus Considerandos 11 y 12:

«(11) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales;
(12) Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de

82 DEL PESO NAVARRO, Emilio (2000). *Ley de Protección de Datos: la nueva LORTAD.* Editorial Díaz de Santos. Madrid. Página 17.

aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones»

1.1 Clasificación de los principios de protección de datos

Para clasificar los principios en esta materia regulados en los artículo 4 a 12 de la LOPD podemos, en primer lugar, atenernos a la clasificación que se desprende de la identificación de las fases del tratamiento y que ya hemos expuesto con anterioridad pero merece la pena proponer una clasificación alternativa, basada en la que en su momento propuso el Ministerio de Justicia durante la presentación de la LORTAD ante el Congreso de los Diputados[83] y que los clasifica en función de su aplicación.

1.1.1 Principios de carácter general

Nos referimos a aquel tipo de principios cuya aplicación es fundamental a lo largo de todas las fases del tratamiento. Hablamos por tanto de los principios de: proporcionalidad, vinculación al fin, exactitud, transparencia así como del secreto del responsable.

1.1.2 Principios especiales

El establecimiento de esta categoría responde al reconocimiento de protección máximo para ciertos datos personales considerados *sensibles.*

1.1.3 Principios singulares

Nos encontramos en presencia de principios que afectan a los momentos muy particulares del tratamiento (recogida, el tratamiento y la utilización): recogida, tratamiento y cesión.
Todos los aspectos de cada uno de los principios que examinaremos a continuación
pueden ser encuadrados de acuerdo con la clasificación expuesta.

83 DAVARA RODRIGUEZ, Miguel Ángel (2006). *Manual de Derecho Informático*. Editorial Thompson Aranzadi. Elcano (Navarra). Página 68

No obstante y a pesar de que esta clasificación no se encuentra falta de cierta utilidad, es preferible utilizar una clasificación más clásica y por la que han optado la mayoría de los autores, basada en aglutinar varios de estos principios en una única categoría. De esta forma obtenemos la presenta clasificación: principio de calidad, principio de información, principio de consentimiento, principio de finalidad del tratamiento, datos especialmente protegidos y principio de seguridad de los datos.

Es básico entender que no nos encontramos ante una serie de principios abstractos, sino que su inobservancia por el responsable del tratamiento constituye una infracción que acarrea, de forma posterior, una sanción.

En esencia, la aplicación de los principios trata de garantizar que los datos de carácter personal:

- Se tratan de manera leal y lícita.
- Se recogen con fines determinados, explícitos y legítimos.
- Son adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad para la cual han sido recabados.
- Su tratamiento responde al consentimiento del afectado.
- Son exactos y se mantienen actualizados de manera que respondan con veracidad a la situación actual del afectado.
- Únicamente se conservan durante el tiempo necesario para cumplir con la finalidad para la cual han sido recogidos.
- Se mantienen bajo unas determinadas condiciones de seguridad.

2. Principio de calidad

El principio de calidad se encuentra regulado en el artículo 4 de la LOPD:

"Artículo 4. Calidad de los datos.

1. 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.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento integro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.»

2.1 Contenido del principio de calidad

El presente principio tiene como misión garantizar la adecuación, exactitud, pertinencia y proporcionalidad de los datos de carácter personal, requisitos que deben cumplirse tanto en el momento de su recogida como a lo largo de todo el tratamiento. Su aplicación deriva en una serie de obligaciones para el responsable del tratamiento. Por lo tanto, cualquier tratamiento de datos personales deberá garantizar que los datos objeto de gestión:

- Son adecuados o pertinentes
- No son excesivos
- Son exactos o actualizados
- Cumplen con el principio de legalidad

2.2 Datos adecuados o pertinentes

Tal y como hemos tenido oportunidad anteriormente, el presente principio establece que los datos solo podrán ser recogidos para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Conviene ahora matizar qué debe entenderse por *datos pertinentes o adecuados*.
Esta exigencia aplica por lo tanto desde el momento de la recogida de los datos. En este sentido, la segunda parte del artículo 4.1 nos ofrece la clave y que se basa en partir de la base de la cualidad del dato personal así como de la finalidad del tratamiento. Asimismo, el Reglamento de desarrollo de la LOPD refuerza esta hipótesis en su artículo 8.3:

«Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos».

2.3 Datos no excesivos

El artículo 4.2 de la LOPD establece:

«Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos»

Topamos en este punto con la referencia a la finalidad de la recogida de los datos como *medida* para evaluar el cumplimiento del principio de calidad. La inclusión de la expresión "*finalidades incompatibles*", fue muy criticada ya que vino a sustituir a la mención incluida en la LORTAD que se refería a finalidades "*distintas*". En este sentido debemos entender que el uso del término "*incompatibles*" -más restrictivo que el anterior- responde a una trasposición apresurada de la Directiva 95/46/CE.

2.4 Datos exactos o actualizados

El artículo 4 de LOPD establece, en sus apartados 3º y 4º:

«3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo».

En este sentido Herrán Ortiz[84] indica que *«la veracidad y exactitud de la información constituye una necesidad para la licitud del tratamiento; un dato personal no puede ser adecuado ni pertinente cuando es inexacto o incompleto, y no responde a la verdadera situación del interesado. No puede ampararse la utilización y el tratamiento de datos personales que no responden con veracidad y exactitud a la situación del interesado, salvo en casos excepcionales donde precisamente el tratamiento se justifique por el carácter histórico de los datos personales».*

84 HERRAN ORTIZ, Ana Isabel (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Dykinson. Madrid.

Por tanto, parece que la LOPD establece la obligación de que el tratamiento de los datos se refiera exclusivamente a datos actualizados, como medio para garantizar los derechos de los afectados. Obligación particularmente importante cuando nos referimos a datos que aluden a determinados aspectos de la personalidad o de la situación social, económica, etc., del titular. Así puede verse en una Resolución[85] de la Agencia Española de Protección de Datos que reflexiona sobre este punto y que fue dictada ante la denuncia interpuesta por un particular por el mantenimiento de sus datos en un fichero de impagados:

«La obligación establecida en el artículo 4 transcrito, impone la necesidad de que los datos personales que se recojan en cualquier fichero sean exactos y respondan, en todo momento, a la situación actual de los afectados, siendo los responsables de los ficheros quienes responden del cumplimiento de esta obligación».

En este sentido el artículo 29 de la LOPD, y que dispone en su apartado 2:

«Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley».

Añadiendo el párrafo 4 del mismo artículo que:

«Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos».

Queda claro pues que es el acreedor el responsable de que los datos cumplan los requisitos establecidos en el artículo 4 de la LOPD, puesto que como acreedor es el único que tiene la posibilidad de incluir los datos en el fichero y de instar la cancelación de los mismos, toda vez que es él el que conoce si la deuda realmente existe o si ha sido saldada o no, siendo las entidades

85 Agencia Española de Protección de Datos (2005). Resolución de 31 de mayo de 2005.

informantes las que deciden a quien dan de alta o de baja, fundamentándose de esta forma la exigencia al responsable del fichero de cancelar y sustituir de oficio los datos inexactos o incompletos por los datos correctos, sin perjuicio de la obligación de garantizar el ejercicio de los derechos de rectificación y cancelación, reconocidos en el artículo 16 LOPD.

De esta forma el legislador establece una doble vía para que pueda garantizarse el cumplimiento de este principio y pese a que la obligación se atribuye legalmente al responsable del fichero que deberá modificar y rectificar los datos personales cuando tenga constancia de su inexactitud, el legislador reconoce al titular de los datos el derecho a instar dicha rectificación o en su caso cancelación de la información, para que actúe y no deje exclusivamente en manos del responsable del tratamiento la verificación y el control de la exactitud y veracidad de los datos personales.

2.4.1 Cumplimiento de la obligación

En este punto merece la pena citar una Sentencia del Tribunal Superior de Justicia de Madrid, de 10 de mayo de 2000[86]:

«La palabra mantener denota una idea de permanencia temporal, por lo que, a juicio de esta Sala y Sección, la acción típica consistirá en la conservación de un dato no actualizado, o, el mantenimiento de un dato erróneo una vez que se tiene conocimiento de su inexactitud».

Por su parte, el Reglamento de desarrollo de la LOPD, artículos 8.5 y 8.6 regula el procedimiento para el cumplimiento de esta obligación:

- Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.
- Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados. En este sentido se establece un plazo de diez días desde que se tuviese conocimiento de la inexactitud, para su cumplimiento.
- En el caso de que los datos inexactos o incompletos hubieran sido comunicados previamente, el responsable del fichero deberá notificar al cesionario -siempre que éste sea conocido-, en el plazo de diez días, la rectificación o cancelación efectuada.

86 Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-administrativo, Sección 8ª, Sentencia de 10 de mayo de 2000. Recurso 1513/1997.

- También se establece un plazo de diez días a contar desde la recepción de la notificación efectuada por el responsable para que el cesionario que mantuviera el tratamiento de los datos, proceda a la rectificación y cancelación notificada.
- La actualización de los datos llevada a cabo a través de este procedimiento no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de sus derechos.

Además, el artículo 8.6 del Reglamento de desarrollo de la LOPD regula también el supuesto de cancelación y bloqueo de los datos personales en aquellos casos en los que los mismos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recogidos. De esta forma, el Reglamento prevé que podrán conservarse los datos 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. Una vez cumplido dicho período, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo establecida en el artículo 16.3 de la LOPD:

«La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión».

2.4.2 Tratamientos para fines históricos, estadísticos o científicos

El artículo 4.2 LOPD conforma una excepción a la obligación de mantener los datos exactos y actualizados cuando el destino de los datos sea su tratamiento con fines "históricos, estadísticos o científicos". El citado precepto establece:

«No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento integro de determinados datos».

Sobre este mismo punto el artículo 9 del Reglamento de desarrollo de la LOPD dispone:

«***Artículo 9. Tratamiento con fines estadísticos, históricos o científicos.***
1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.
Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.
2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior».

2.4 Cumplimiento del principio de legalidad

El artículo 4.7 de la LOPD establece una cláusula de cierre por la cual se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Merece la pena detallar un poco más estos tres términos:

- **Medios ilícitos:** Aquellos que resulten contrarios al derecho y que, por lo tanto, sean sancionables.
- **Medios engañosos o fraudulentos:** Aquellos que inducen al engaño o confusión en el titular de los datos o en un tercero con el único objeto de obtener determinados datos del mismo.
- **Medios desleales:** Tal y como establece el Considerando 38 de la Directiva 95/46/CE: *«considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de*

ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención».

No existirá lealtad, por lo tanto, cuando los datos se recojan de forma que los interesados desconozcan el tratamiento o, conociéndolo, carezcan de información precisa acerca del mismo[87].

3. Principio de información

Pilar fundamental de la protección de datos de carácter personal dado que es la única vía para que el interesado pueda conocer quienes son las entidades que van a llevar a cabo el tratamiento de sus datos, con que fines y bajo qué condiciones. Por esta razón, la LOPD establece una serie de garantías que aseguran, al interesado, el ejercicio de sus derechos en esta materia así como la posibilidad de proteger la información que le concierne. El principio de información se encuentra regulado en los artículos 5 de la LOPD y 18 y 19 del su Reglamento de desarrollo:

*«**Artículo 5 LOPD. Derecho de información en la recogida de datos.***

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

87 SANCHEZ MOURIZ, Nelly (2004). *Los datos personales en el inicio de una actividad empresarial. La Protección de Datos en la Gestión de Empresas*. Editorial Thompson Aranzadi. Cizur Menor (Navarra). Página 58.

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.»

*«**Artículo 18 Reglamento de desarrollo de la LOPD. Acreditación del cumplimiento del deber de información.***

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales».

*«**Artículo 19 Reglamento de desarrollo de la LOPD. Supuestos especiales.***

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre».

3.1 Fundamento del principio de información

Su origen se encuentra en los artículos 10 y 11 de la Directiva 95/46/CE. En este sentido, el legislador español, decidió fusionar ambos preceptos en uno solo. El artículo 5 de la LOPD -apartados 1, 2 y 3-, contempla la información respecto de los datos obtenidos del propio interesado, mientras que los apartados 4 y 5 lo hace respecto de obligaciones derivadas de este principio, tal y como establece además, nuestro Tribunal Constitucional[88]:

"Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 C.E.
Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (…), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.
A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos".

3.2 Contenido

3.2.1 Datos obtenidos directamente de los titulares

El artículo 5.1 de la LOPD delimita el principio de información al establecer la obligación general de informar a todos aquellos interesados a los que se les soliciten datos personales: de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa

88 Tribunal Constitucional. Sentencia número 292/2000, de 30 de noviembre.

a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición así como de la idEntidad y dirección del responsable del tratamiento o, en su caso, de su representante.

No obstante el propio artículo 5 de la LOPD dispone una excepción a este deber de información en los casos en los que el contenido de esta información se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. En este sentido la Agencia Española de Protección de Datos, en su Memora de 1995[89] afirmaba:

«La ley otorga una importancia excepcional al principio de autodeterminación informativa, que consiste en el derecho a estar informado del tratamiento de los datos personales por el propio afectado y a otorgar el consentimiento en aquellas situaciones en que la ley lo exija. Por esta razón, la excepción del apartado 3 del artículo 5, que exime del deber de facilitar esta información cuando el contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en las que se recaban, ha de interpretarse de modo notablemente restringido, ya que un consentimiento consciente e informado por parte del afectado se gesta en la recogida de los datos».

La aplicación de este criterio puede verificarse en la jurisprudencia y así podemos señalar como ejemplo el caso de la Sentencia del Tribunal Superior de Justicia de Madrid, de 17 de mayo de 2001[90], en la que se señala:

«Ese deber de información que, en principio, pesa sobre "Telefónica" en la medida que al contratar la prestación del servicio telefónico recaba - y obtiene - los datos personales del cliente relativos a su nombre, apellidos, dirección, sólo quedaría excluido - apartado 3 del artículo 5 - si el contenido de la información que ha de suministrarse "se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban" y el Tribunal no advierte que del contrato de adhesión que suscribe el cliente de "Telefónica" para la obtención de un servicio de telefonía y de los datos que, para ello, tiene que suministrar se deduzca que "Telefónica" tenga un fichero automatizado de datos de carácter personal en el que se van a registrar los datos del cliente, quiénes son los destinatarios de la información de este fichero, el

89 Agencia Española de Protección de Datos. *Memoria 2005* [en línea]. Disponible en: http://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2005/common/pdfs/8290-CAP.IV-Csdigos-Tipo.pdf

90 Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-administrativo, Sección 8ª, Sentencia de 17 de mayo de 2001. Recurso 724/1998.

titular del mismo, la existencia de derechos de acceso, cancelación o rectificación».

En cuanto a la **forma** en la que debe recogerse la información, las obligaciones pueden resumirse en los siguientes puntos:

- La información debe facilitarse de modo "expreso, preciso e inequívoco".
- En cuanto a la forma, no se establece más obligación que exigir en los casos en los que se utilicen cuestionarios o impresos para la recogida, la información figure en forma claramente legible.
- En cuanto al momento de cumplir con la obligación de informar, se exige que este deber se cumpla de forma previa a la recogida.

En este punto debemos tener en cuenta que no encontramos en presencia de una obligación ineludible del responsable del fichero o tratamiento y corresponde a este la carga de la prueba de su cumplimiento.

3.2.2 Datos obtenidos de terceros

En muchas ocasiones, los datos se obtienen de otras entidades o de fuentes accesibles al público y para estos casos los apartados 4 y 5 de la LOPD prevén la forma en la que deberá cumplirse con este principio. El apartado 4º establece un plazo de **tres meses** desde el momento de registro de los datos para que el responsable del fichero informe de forma expresa, precisa e inequívoca[91]: de la identidad del responsable del tratamiento y de su dirección, de la procedencia de los datos, 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, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición así como de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Esta obligación deberá cumplirse siempre que al interesado no se le hubiera informado con anterioridad. De esta forma, las entidades cuyos ficheros contienen datos que no han sido obtenidos directamente de los interesados no estarán obligadas a informar si la persona que recogió los datos ya les hubiera informado.

91 Salvo que el titular ya hubiera sido informado con anterioridad.

Sobre esta regla general se establecen una serie de excepciones en el artículo 5.5 de la LOPD y, `pr tanto, no será de aplicación la obligación que acabamos de ver si:

- Expresamente una ley prevea la excepción.
- El tratamiento tiene fines históricos, estadísticos o científicos.
- 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.
- 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.

Además, el Reglamento de desarrollo de la LOPD -artículos 153 a 156- establece un "Procedimiento de exención del deber de información al interesado", que trata de establecer los medios para evitar la vulneración de los derechos de los titulares, compatibilizándolo con la dificultad para una información en los términos que exige de forma genérica el principio de información. Dicho procedimiento puede resumirse de la siguiente forma:

- **Inicio del procedimiento.** El procedimiento se iniciará siempre a solicitud del responsable del fichero, que entre otros aspectos, deberá:
  - Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.
  - Exponer detalladamente las **medidas compensatorias** que propone en caso de exoneración de la obligación de informar,
  - Aportar una cláusula informativa que, mediante su difusión, permita compensar la exención del deber de informar.
- **Propuesta de nuevas medidas compensatorias**. La Agencia Española de Protección de Datos podrá proponer medidas adicionales si considerara insuficientes las propuestas por el responsable del fichero.
  - Se establece un plazo de 15 días para el traslado de esta resolución al responsable, de forma que este pueda realizar sus alegaciones.
  - El **plazo máximo** para que la Agencia Española de Protección de Datos pueda resolver será de seis meses. Transcurrido dicho plazo, el afectado puede considerar admitida su

solicitud por silencio administrativo positivo.

Otra novedad incorporada por el Reglamento de desarrollo de la LOPD es su artículo 19 que dispone que en los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación societaria[92], no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la LOPD.

3.2.3 Forma de acreditar el cumplimiento de la obligación de informar

Sobre el responsable del tratamiento recae la carga de la prueba acerca del cumplimiento de la obligación de informar. Esta obligación, que ya existía anteriormente a la entrada en vigor del Reglamento de desarrollo de la LOPD, ha sido reforzada por esta norma que en su artículo 18 ha introducido dos obligaciones adicionales que vienen a completar el régimen de garantías establecido a estos efectos:

- El medio utilizado para informar deberá permitir acreditar el cumplimiento de la obligación.
- Estos medios deberán conservarse mientras persista el tratamiento de los datos del afectado. Esto implica conservar el soporte en el que conste el cumplimiento pudiendo utilizarse para ello medios informáticos o telemáticos[93].

La presente regulación recoge en parte la interpretación de la Agencia Española de Protección de Datos a lo largo de los años[94]:

«La Audiencia Nacional ha analizado el efecto probatorio de la notificación a los interesados del tratamiento de sus datos personales en su Sentencia de 24 de enero de 2003, de la que se desprenden las siguientes consecuencias:

- La mera contratación de un medio independiente para la notificación no acredita más que la

92 Fusión, escisión, cesión global de activos y pasivos, etc.

93 El artículo 18 Reglamento de desarrollo de la LOPD admite expresamente la utilización de sistemas de escaneado de la documentación en soporte papel, "siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales"

94 Agencia Española de Protección de Datos (2007). Informe 0020/2007 [en línea]. Cumplimiento del deber de información Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/deber_informacion/common/pdfs/2007-0020_Cumplimiento-del-deber-de-informaci-oo-n.pdf [2010, 15 de junio]

existencia del contrato, pero no que se ha hecho el envío.

- La prueba del envío de una notificación no acredita por sí misma su recepción por el afectado.

- Si el destinatario niega la recepción, la carga de la prueba del envío recae sobre el responsable del tratamiento.

- El que se hayan efectuado otras notificaciones al afectado no es suficiente para probar la notificación del "documento" respecto del cual se niega la recepción.

En consecuencia, la Audiencia Nacional viene a reconocer ***que sin perjuicio de que la carga de la prueba de la notificación corresponde al responsable del fichero, será suficiente para lograr esa acreditación la aportación de indicios suficientes que coadyuven a entender cumplido el requisito.***

Ciertamente, los posibles indicios a aportar podrán diferir en cada caso En el supuesto analizado por la Sentencia de 31 de mayo de 2006, se aceptaron como indicios "la inclusión en el fichero auxiliar de notificaciones de esta comunicación como realizada" y el hecho de que "(el afectado) se dirige a (la recurrente) sabiendo que sus datos están incluidos en el fichero y quien había sido la Entidad informante de los mismos sin que se haya acreditado mínimamente que dicho conocimiento lo obtuvo de forma distinta de la comunicación que dice haber realizado (la recurrente), y, finalmente, "el hecho de que al domicilio al que aparece dirigida la comunicación que se niega haber recibido, se han remitido otras comunicaciones de las que el denunciante ha tenido perfecto conocimiento".

No obstante, podría resultar conveniente la utilización de medios fiables, independientes y auditables para la realización de las notificaciones o la obligación de comprobación de que los envíos no han sido devueltos por su destinatario. Al tratarse de medios independientes, en el caso planteado, resultaría aconsejable que la acreditación de dichos envíos y las posibles devoluciones las efectuará una persona distinta al Secretario General del Colegio»

4. Principio de consentimiento

El principio del consentimiento se encuentra regulado en el artículo 6 de la LOPD:

«***Artículo 6. Consentimiento del afectado.***

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal 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 en los términos del artículo 7, apartado 6, de la presente Ley, o 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.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

El régimen de protección establecido por nuestro ordenamiento para los datos de carácter personal gira en torno al consentimiento del afectado. Así, para Lucas Murillo de la Cueva[95] «*el consentimiento del afectado es la piedra angular a partir de la cual se construye el sistema de protección de datos personales frente al uso de la informática*».

95 MURILLO DE LA CUEVA. Pablo Lucas (1990). *El Derecho a la Autodeterminación Informativa. La Protección de Datos Personales frente al Uso de la Informática*. Editorial TECNOS. Madrid.

En idéntico sentido se pronuncia Serrano Pérez[96], indica:

«A nuestro juicio, el derecho a la libertad informática o protección de datos, del art. 18.4 de la constitución, como derecho desarrollado por la LOPD, se sustenta sobre dos pilares fundamentales: el consentimiento y el conjunto de derechos que lo hacen practicable.
El primero de ellos se manifiesta como autodeterminación del individuo y conforma el espacio de libertad y dignidad de la persona, junto con el resto de los derechos fundamentales. El segundo de ellos, los derechos que lo hacen practicable, determina las facultades que posibilitan el ejercicio del derecho fundamental y garantizan su protección. Ambos constituyen el contenido esencial del derecho a la protección de datos siendo, por tanto, un límite absoluto e intocable ante la acción del legislador».

Por su parte, para Almuzara Almaida[97]:

«E*l principio de consentimiento es uno de los pilares en los que, junto con la finalidad se asientan las bases principales de la regulación normativa de la Ley Orgánica 15/1999, al igual que su antecesora, la Ley Orgánica 5/1992».*

Esta importancia se deja notar también en la Sentencia del Tribunal Constitucional 292/2000, de 30 de Noviembre:

"(…) El derecho fundamental a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos (…) y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento pata la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos, En definitiva, el poder de disposición sobre los datos personales.»

96 SERRANO PÉREZ, María Mercedes (2003). *El derecho fundamental a la protección de datos. Derecho español y comparado*. Editorial Thomson Civitas. Madrid.
97 ALMUZARA ALMAIDA, C. (Coord.) (2005). *Estudio Práctico sobre la protección de datos de carácter personal*. Editorial Lex Nova. Valladolid.

Siguiendo a APARICIO SALOM[98], se entiende que el tratamiento de datos de carácter personal constituye una relación jurídica en cuyo estudio el consentimiento es la pieza clave para determinar su naturaleza. En este sentido, el artículo 6.1 plantea dos posibles situaciones en el tratamiento de los datos:

- Tratamiento de datos consentido por el titular de los mismos. En este caso es el resultado de la manifestación de la voluntad de las partes. Por un lado, el responsable del fichero que lo ofrece, y por otro, el titular de los datos, que lo acepta.
- Tratamiento de datos no consentido por el titular de los mismos. Nace como consecuencia de una ley y supone la obligación del responsable del fichero de mantener el tratamiento durante el tiempo y con los requisitos derivados de la norma que lo autoriza.

Dentro del segundo grupo, también es posible incluir los supuestos recogidos en el artículo 6.2 en los que "*no será preciso el consentimiento*" para proceder al tratamiento de los datos:

- Datos recogidos por las Administraciones públicas en el ejercicio de sus funciones, cuyo tratamiento quedará habilitado en la mayor parte de los casos "ley" entiendo este término en el sentido amplio de norma jurídica.
- Datos que 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. En estos casos, en realidad, el consentimiento al tratamiento de los datos sí existe, puesto que se deriva como consecuencia lógica del consentimiento prestado para la obligación principal. Tal y como establece el artículo 15 del Reglamento de desarrollo de la LOPD, en el caso de que el responsable del fichero desee aplicar los datos a finalidades diferentes de las estrictamente derivadas del mantenimiento y gestión del contrato o precontrato, deberá informar al interesado de las mismas, y facilitar un mecanismo que le permita manifestar expresamente su negativa al tratamiento o comunicación de datos. Dicho artículo continúa diciendo que se entenderá cumplido estos deberes facilitando la posibilidad de marcar una casilla en el documento que se entregue en la celebración del contrato.
- Datos tratados con la finalidad de proteger un interés vital del interesado.
- Datos que 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

98 APARICIO SALOM, Javier (2000). *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal.* Editorial Aranzadi. Elcano (Navarra). Páginas 27 a 31.

tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

4.1 Definición de consentimiento

El consentimiento es «*Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*»**.**

De la presente definición se pueden deducir cuatro características que fueron objeto de análisis en la Memoria de la Agencia del año 2000[99]:

«a*) **Libre,** lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.*
*b) **Específico,** es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999.*
*c) **Informado,** es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.*
*d) **Inequívoco,** lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia **del consentimiento.**»*

99 Agencia Española de Protección de Datos. *Memoria del año 2000* [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2000/common/pdfs/MemoriaApd2000.pdf

4.2 Tipos de consentimiento

En este punto debe hacerse referencia a la doctrina civil, para la que el consentimiento, como manifestación de voluntad, puede ser expreso, presunto y tácito.

Siguiendo al profesor ALBALADEJO podemos extraer las definiciones de manifestaciones expresas, presuntas y tácitas:

- **Declaración expresa:** «*Es aquella realizada con medios que por su naturaleza están destinados a exteriorizar la voluntad (medios objetivos de declaración), como la palabra, el escrito, etc.*.».
- **Declaración tácita:** «*Consiste en un comportamiento (hechos concluyentes: facta concludentia), que sin ser medio destinado por su naturaleza a exteriorizar la voluntad, la exterioriza, sin embargo, porque a través de él se advierte que el sujeto que lo realiza tiene una voluntad determinada.*»
- **Declaración presunta:** «*Háblase de declaraciones presuntas en los casos en que el derecho considera a cierto comportamiento (que no encamina a declarar, que no es, por su naturaleza, medio de declaración) como declarativo de una determinada voluntad, es decir, la ley dispone que una conducta determinada debe ser considerada como declaración de tal o cual voluntad. Se dice entonces que la ley deduce o presume la voluntad. Y la conducta que da base para tal presunción, se califica de declaración presunta.*»

Siguiendo esta doctrina, la Agencia Española de Protección de Datos indicó en su Memoria del año 1994[100]:

«El consentimiento expreso se manifiesta como un acto positivo y declarativo de la voluntad.
El consentimiento tácito se produce cuando, pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo. Es decir, cuando el silencio se presume como un acto de aquiescencia o aceptación.
El consentimiento presunto es aquél 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»

100 Agencia Española de Protección de Datos. *Memoria del año 1994* [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_1994/common/pdfs/MemoriaApd1994.pdf

En relación a los datos calificados como especialmente protegidos, la normativa -artículo 7 de la LOPD- impone un régimen reforzado para su tratamiento que, entre otros aspectos, implica la **obligación de que el consentimiento sea expreso** en el caso de la recogida de estos datos:

- Los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias requerirán el consentimiento expreso y por escrito del titular de los mismos, que deberá ser previamente informado por el responsable del fichero de su derecho a negarse a facilitar dichos datos.
- 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. Tal y como establece el artículo 7.6 de la LOPD los datos podrán ser tratados sin consentimiento del interesado «*cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.*»

En el resto de los supuestos, el consentimiento podrá ser expreso, presunto o tácito. Con la entrada en vigor de la LOPD, se planteó la duda de si la exigencia de que el consentimiento sea inequívoco excluye la posibilidad de solicitarlo tácitamente. En este sentido, APARICIO SALOM indica:

«Por último, para terminar con el estudio del consentimiento tácito, debe atenderse al tenor literal del artículo 6.1 de la LOPD que establece que el consentimiento para el tratamiento debe ser inequívoco, a diferencia de la LORTAD, que no utilizaba ningún adjetivo para designar el consentimiento necesario para la licitud del tratamiento. Esta especificación se ha introducido conforme al proyecto de Ley Orgánica de Reforma elaborado por el Gobierno. La exigencia de que el consentimiento sea inequívoco, no parece añadir ningún requisito adicional a su exigencia, ni contradecir la admisión del consentimiento tácito que se establece en la nueva LOPD.

El significado semántico de inequívoco supone que en ese precepto se exige que el consentimiento otorgado no admita duda, esto es, que sólo puede ser entenderse autorizado aquello que, efectivamente, no puede dudarse de que se consistió. En definitiva cuando la ley exige que el consentimiento sea inequívoco, no se está refiriendo a la forma en que puede otorgarse o

manifestarse, sino a su contenido, a la voluntad de autorizar el tratamiento, lo que supone, por tanto, que la Ley exige una interpretación restrictiva del consentimiento otorgado. No cabe por ello identificar consentimiento inequívoco con consentimiento expreso, ya que esta última expresión se refiere, no al contenido del consentimiento, sino a la forma de otorgarlo».

4.3 La obtención del consentimiento

4.3.1 Medios de obtención del consentimiento

El consentimiento puede obtenerse a través de cualquier medio por el que el interesado deje constancia de su manifestación de voluntad. Los cauces más utilizados para la obtención del consentimiento son el escrito, con firma del interesado, la palabra, generalmente con grabación de voz del titular de los datos, y la aceptación de cláusulas informativas en Internet. Con excepción de los datos especialmente protegidos, la LOPD no exige que éste haya de otorgarse de una manera concreta, ni impone que sea por escrito. Sin embargo, como señala Almuzara Almaida la forma escrita es el medio que ofrece mayores garantías a la hora de probar la obtención del consentimiento:

«Indudablemente es el medio más idóneo para la acreditación del cumplimiento de los principios de información y consentimiento por parte del responsable del fichero, máxime si se obtiene de forma expresa, es decir, acompañado de la firma del titular de los mismos.
No obstante, debe retenerse en cuenta que, el responsable del fichero o tratamiento deberá igualmente custodiar con suficiente diligencia dicha documentación, dado que en el supuesto de solicitud por parte de la Agencia Española de Protección de Datos deberá presentar dicha documentación.

Los responsables de los ficheros deben igualmente ser diligentes y consecuentes con el consentimiento otorgado por su titular. En este sentido, determinados responsables de ficheros han sido objeto de sanción al no actuar con suficiente cuidado en la tramitación de los términos de la autorización otorgada por su titular. En este sentido, no basta con realizar una adecuada formulación del derecho de información y de la solicitud del consentimiento, además, éste deberá ser adecuadamente tratado.»

El medio oral plantea el problema principal de articular mecanismos de prueba, como la grabación

de conversaciones que en muchas ocasiones resultan inviables o demasiado costosa.

En relación a la recogida del consentimiento a través de Internet, el Informe Jurídico de la Agencia Española de Protección de Datos 49/2007[101] expone las siguientes reglas:

«En el supuesto de que la recogida de datos se realice a través de una página web, las obligaciones a las que acabamos de referirnos, suelen cumplirse mediante formularios y cláusulas a los que se accede a través de enlaces como pueden ser "aviso legal" o "política de protección". También es importante incluir algún tipo de "link" de este tipo en relación con los derechos de los interesados de rectificación, cancelación, acceso y oposición.
En cuanto al consentimiento informado, este habrá de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco tal y como exige la Ley.»

Para finalizar este apartado, debemos señalar que el medio que el responsable del fichero elija para recabar el consentimiento dependerá, fundamentalmente, de dos cuestiones:

- Del tipo de consentimiento que desee recabar (expreso, presunto o tácito). En el caso de los datos especialmente protegidos, sólo podrá ser expreso, sin que quepa deducirse de su silencio.
- Las garantías de prueba que desee obtener. Simplemente recordar que los principios de información y consentimiento, aunque distintos, se configuran en nuestra normativa como dependientes, de tal manera que en muchos casos, bastará con probar que se informó del tratamiento al interesado y que éste no se opuso.

4.3.2 Procedimiento para la obtención del consentimiento presunto

Debido a la confusión general existente entre tipos de consentimiento y medios de expresión de la

101 Agencia Española de Protección de Datos (2007). Informe 0049/2007 [en línea]. *Tratamiento de datos a través de páginas web*. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2007-0049_Tratamiento-de-datos-a-traves-de-p-aa-ginas-web.pdf [2010, 16 de junio]

manifestación de la voluntad en que consiste el consentimiento, se plantearon diversas dudas sobre la posibilidad de obtención del consentimiento tácito en determinados tratamientos. Con objeto de solventar los problemas surgidos entorno a esta figura, el Reglamento de desarrollo de la LOPD dedica su artículo 14 a la descripción del procedimiento que deberán seguir aquellos responsables de fichero que deseen obtener el consentimiento tácito de los titulares de los datos.

Este procedimiento se encuentra enfocado a la obtención del consentimiento tácito[102] por correo postal u ordinario, siendo obligación del responsable del tratamiento:

- Informar al interesado en los términos previstos del artículo 5 de la LOPD y, de forma adicional:
  - Que dispone de un plazo de treinta días para manifestar su negativa.
  - Que en caso de no hacerlo, se entenderá que consiente al tratamiento.
- Si la información se le remite en los envíos periódicos de facturas, deberá aparecer siempre de forma clara.
- El medio utilizado para el envío que haga el responsable del fichero habrá de permitir controlar las devoluciones.
- Facilitar al interesado un medio sencillo y gratuito para manifestar su negativa.

4.3.3 Obtención del consentimiento de menores e incapaces.

Tal y como establece Aparicio Salom, «*la capacidad necesaria para aceptar la relación jurídica para consentir el tratamiento de los datos, es la capacidad general necesaria para la eficacia de los actos jurídicos (…)*».

No debemos olvidar que este concepto se refiere a personas incapacitadas legalmente tal y como establece el artículo 200 del Código Civil: «*Son causas de incapacitación las enfermedades o deficiencias persistentes de carácter físico o psíquico que impidan a la persona gobernarse por sí misma*».

No obstante, el caso de los menores de edad ha suscitado dudas, habida cuenta de que la minoría de edad no supone una causa de incapacitación y deberá ser analizada en cada caso concreto para

102 Debe tenerse en cuenta que esta forma de obtención del consentimiento está limitada a un plazo de temporal de ejercicio ya que sólo podrá utilizarse una vez al año sobre los mismos tratamientos y para las mismas finalidades.

poder calificar la suficiencia en la prestación del consentimiento en relación a la trascendencia del acto de disposición y a la madurez del menor. En este sentido, el artículo 13 del Reglamento de desarrollo de la LOPD diferencia entre los menores de edad que superan los 14 años y aquellos que no:

- Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.
- En el caso de menores de 14 años, deberá contarse en todo caso con el consentimiento de padres o tutores.

Por tanto, cuando se recabe el consentimiento de un menor, los datos que se soliciten deberán referirse únicamente a su persona, no a sus padres o a hábitos de su grupo familiar. Además, para entender el consentimiento válidamente prestado, deberá haberse informado al menor de las condiciones del tratamiento en un lenguaje sencillo de forma que éste lo pueda comprender.

4.4 Revocación del consentimiento

El artículo 6.3 de la LOPD establece: *«El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos»*.

La LOPD confiere a los interesados una facultad de revocar el consentimiento otorgado. Esta posibilidad de revocación presupone que el consentimiento haya sido prestado, por lo tanto no será de aplicación a aquellos supuestos en los que el tratamiento se realice sin consentimiento del interesado. En estos casos se ofrece la posibilidad de ejercer el derecho de oposición, tal y como establece el artículo 6.4 de la LOPD:

«En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado».

Por su parte, el artículo 17 del Reglamento de desarrollo de la LOPD nos aporta algunos datos adicionales y que deben ser tenidos en cuenta:

- **Modo en que debe ejercerse la petición**: Será fijado por el Responsable del tratamiento, que deberá habilitar un medio sencillo, gratuito y que no implique ingreso alguno para él mismo, como por ejemplo: envío de carta prefranqueada, llamada a un número de teléfono gratuito, llamada al servicio de atención al público de la Entidad. En todo caso, se prohíbe expresamente imponer al interesado el ejercicio de esta facultad de revocación a través de dos mecanismos: el correo certificado o equivalente y los servicios de telecomunicaciones que impliquen tarifación adicional.
- **Plazo en que debe hacerse efectiva la petición**: Se fija el plazo máximo de 10 días, a contar desde la recepción de la petición.
- **Efectos de la revocación**: El resultado del ejercicio de esta facultad supondrá que el Responsable del Fichero cesará en el tratamiento de los datos. Este cese en el tratamiento no implica, de forma necesaria, el borrado físico de los datos, sino que éstos podrán bloquearse, manteniéndose a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Sólo será necesario responder expresamente a la petición del interesado si éste lo solicita. Sin embargo, el responsable del tratamiento sí deberá comunicar a todos los cesionarios de datos en el mismo plazo de 10 días hábiles a que nos hemos referido, que el consentimiento ha sido revocado para que éstos cesen a su vez en el tratamiento de los datos.

5. Finalidad

El principio de finalidad es, junto con el del consentimiento, uno de los pilares fundamentales en la regulación del derecho a la protección de los datos de carácter personal. Establecido en el artículo 4.2 LOPD, establece que los datos de carácter personal no pueden utilizarse para fines incompatibles con aquellos para los que hubiesen sido recogidos.

En este sentido merece la pena poner en relación el concepto de "*finalidades incompatibles*" con el principio de autodeterminación, que implica que el afectado conozca o pueda conocer, mediante el empleo de una diligencia razonable, que los datos por él facilitados van a ser empleados para los fines para los cuales dichos datos han sido recabados. Por tanto, los datos recabados por parte de la Entidad deben contar con una justificación, acorde con la finalidad para la que vayan a ser utilizados y, por supuesto, respetando la legalidad del resto de principios.

En este sentido el artículo 4.2 de la LOPD dispone que:

«Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.»

Por su parte el 4.5 de la LOPD establece:

«Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento integro de determinados datos.

5.1 El principio de finalidad

En atención a la finalidad por la que se realiza el tratamiento, este puede resultar legítimo o ilegítimo. Tal y como establece el artículo 4.2 de la LOPD los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Merece la pena profundizar en el concepto de *finalidad incompatible* ya que supone la clave de este artículo 4.2 de la LOPD.

La LOPD modificó sustancialmente la LORTAD que en su artículo 4 recogía la mención "*finalidades distintas*". Nuestra Audiencia Nacional, en sentencia de 8 de febrero de 2006[103] estableció una interpretación sobre el artículo 4.2 de la LOPD:

«(…) aunque el artículo 4;2 *de la Ley* 15/99, *en contraposición con el artículo* 4.2 *de la Ley* 5/92, ya *no* se *refiere* a *"finalidades distintas': sino* a *"finalidades incompatibles': revelando una ampliación de la posibilidad de utilización de los datos, sin embargo la interpretación sistemática del precepto* y *la ambigüedad del término '1inalidades incompatibles" avalan la interpretación realizada en el acto administrativo impugnado.*

En efecto, según el diccionario de la Real Academia "incompatibilidad" significa "repugnancia que tiene una cosa para unirse con otra, o *de dos* o *más personas entre sí", por tanto, una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida* e *ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que "semejante interpretación conduce al absurdo* y *como tal ha de rechazarse", como hemos declarado en Sentencia de* 8 *de febrero de 2002.*

Teniendo en cuenta, además, que dicho término se introduce en el Ley de 1999, *como ha declarado la doctrina, por una traducción poco precisa del artículo* 6 *de la Directiva* 46/1995, *de* 24 *de octubre.*

Conclusión igualmente avalada por la interpretación sistemática aludida, pues como señalamos en la citada Sentencia de 8 *de febrero de 2002, "semejante prescripción no puede ser entendida sino como un enunciado de carácter general, que no puede prevalecer sobre la regulación específica de una materia"' citando al efecto el artículo* 6 *de la citada Ley, y añadiendo que la interpretación de dicho artículo* 6.2, a *sensu contrario, impone "que cuando los datos* se *usen con otra finalidad distinta se precisará el consentimiento del afectado.*

103 Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 8 de febrero de 2006. Recurso 495/2004.

Y no parece que el artículo 4.2, *venga* a *efectuar una ampliación sobre la posibilidad de utilización de los datos, como entiende el actor, porque ello supondría dejar sin contenido el art* 6.2, *cuya redacción en este punto es igual* a su *homónimo de la Ley* 5/92».

En base a la citada sentencia, la interpretación al término "*finalidad incompatible*", debe de ser necesariamente restrictiva para evitar que cualquier tipo de finalidad pudiera ampararse en una indefinición de este concepto. Parece pues claro que el principio de finalidad implica que el afectado tenga la garantía de que los datos por él facilitados van a ser empleados en consonancia con los fines para los que los facilita. Esta interpretación también puede encontrarse, nuevamente, en la jurisprudencia de nuestra Audiencia Nacional[104]:

«(…) *mostrando en definitiva tal artículo 4 de la LOPD una sutil distinción entre finalidad de la recogida y finalidad del tratamiento, pues la recogida sólo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines.*
Así pues, y de acuerdo con el artículo 1.b) de la Directiva 95/46/CE de 24 de octubre de 1995 (en cuya redacción se inspira el repetido artículo 4.2 de nuestra LOPD), si la recogida se hizo con fines determinados, cualquier uso o tratamiento posterior con finalidad distinta es incompatible con la primera finalidad que determinó la captura por lo que, en este contexto, diferente o incompatible significan lo mismo.»

En conclusión, los datos no pueden ser tratados para fines incompatibles o distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado. En este mismo sentido, podemos citar otras sentencias, como la Sentencia de 8 de febrero de 2006[105], de la Audiencia Nacional que señala como, el artículo 4.2 de la LODP impide la utilización de los datos *«para un fin incompatible con el derivado del interés apreciado para acceder al Registro, debiendo recordarse que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, ha venido a sentar la doctrina de que el término "incompatible" debe ser interpretado restrictivamente, debiendo considerarse, con carácter general, asimilado a "distinto"»*.

104 Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 15 de junio de 2005. Recurso 669/2003.
105 Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 8 de febrero de 2006. Recurso 495/2004.

5.2 Aplicación

5.2.1 Consentimiento

Ya hemos visto anteriormente que el tratamiento de los datos personales requiere siempre el consentimiento inequívoco del afectado, debiendo tener en cuenta que una finalidad distinta o incompatible implica un nuevo tratamiento. Una vez aplicado el criterio restrictivo en la determinación de la existencia de una nueva finalidad incompatible con la que motivó la recogida de los datos, será necesario contar con el consentimiento para esta nueva finalidad. En palabras de la propia Agencia Española de Protección de Datos[106]:

«No se recabarán datos personales cuyo conocimiento por parte del responsable no esté justificado por las finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado. En particular, no se recabarán datos personales a través de líneas 906 cuando éstos no vayan a ser utilizados para la finalidad comunicada y su recogida sólo esté motivada por cuestiones promocionales.

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que haya justificado su recogida. A este respecto debe recordarse que la Sentencia 292/2000 del Tribunal Constitucional ha señalado que "el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros (…). Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatible con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado". Así para que tales datos puedan ser usados para una finalidad distintas, es imprescindible obtener previamente el consentimiento inequívoco del afectado».

106 Agencia Española de Protección de Datos. Inspección sectorial de oficio "Concursos, juegos y sorteos de televisión". Conclusiones y Recomendaciones. Octubre de 2002

5.2.2 Información

El artículo 5.1 LOPD exige que los afectados o interesados, a los que se soliciten datos personales, estén previamente informados de modo expreso, preciso e inequívoco, entre otros aspectos, de la finalidad de la recogida de éstos.

Por tanto, el cumplimiento del principio de finalidad, exige que en el momento de la información del titular, se informe al titular de los datos sobre la finalidad concreta del tratamiento de datos que se pretende llevar a cabo siendo necesario evitar las referencias a finalidades genéricas e indeterminadas. Debemos poner en relación este deber de información con el artículo 11 de la LOPD, dedicado a las comunicaciones de datos, y que establece en su primer apartado:

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

En este sentido es necesario remitirse a las consideraciones realizadas por la Agencia Española de Protección de Datos en sus Recomendaciones emitidas en relación con la gestión de tarjetas utilizadas en las grandes superficies comerciales:

«En consecuencia, cuando las entidades a las que afecta esta recomendación comuniquen o cedan los datos personales recabados de sus clientes a otras empresas del grupo de sociedades al que pertenezca el establecimiento financiero o centro comercial, deberán cumplir acumulativamente las dos acciones impuestas por el trascrito artículo 11.1.
Además la finalidad de la cesión ha de ser cognoscible para el interesado en el momento de prestar el consentimiento, no siendo lícito el mero consentimiento genérico para ceder sus datos conforme a expresiones tales como "ceder sus datos a otras empresas del grupo", "realizar publicidad", "remitirles ofertas comerciales …".
En definitiva, el consentimiento ha de otorgarse para supuestos y finalidades concretas y determinadas, siendo nulo de pleno derecho, de conformidad con lo dispuesto en el artículo 11.3 de la misma Ley, el consentimiento para la cesión absoluta o indeterminada».

En relación a las obligaciones ligadas al principio de finalidad, la Memoria del año 2000 de la Agencia Española de Protección de Datos establece varias cuestiones de interés que se hace necesario analizar, en relación a un estudio llevado a cabo a raíz de una consulta realizada por una Entidad financiera con relación al cambio de finalidad en el tratamiento y cesión de datos a las empresas participadas dentro de su mismo grupo. La Agencia Española de Protección de Datos pone de manifiesto en esta consulta la disconformidad con la comunicación cursada por una Entidad bancaria a sus clientes, en la que se informaba del nuevo tratamiento que se iba a realizar con sus datos personales, así como de la posibilidad de cesión de los mismos a las entidades del grupo o a entidades participadas:

"A la vista de las disposiciones anteriores (artículos 4.1, 4.2 y 6.1 LOPD) se desprende que la actuación de la Entidad bancaria respecto del nuevo tratamiento, podría ser conforme a derecho, dado que al variar la finalidad del tratamiento de los datos de sus clientes con el objeto de mejorar la promoción comercial de sus propios servicios, les está solicitando a cada uno de ellos el consentimiento para poder realizar dicho tratamiento, situación acorde con lo que establecen dichos preceptos.

Respecto de la cesión de sus datos se le señaló, al igual que en el caso del grupo eléctrico anteriormente expuesto, que la LOPD dentro de su artículo 11 regula la comunicación de datos, estableciendo el principio de que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

No obstante, el propio artículo 11 establece que, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar. En este sentido se le señala que la finalidad deberá ser determinada, explícita y legitima.
Del contenido de la carta enviada por la Entidad bancaria, no se podía apreciar por los clientes, la finalidad explícita, determinada y legítima a la que se iban a destinar los datos, ni tampoco quedaban determinados los destinatarios de la cesión, por lo que en principio, dicha comunicación no tendría validez.

A estos efectos y dado que la carta anterior carecería de validez en la parte de la cesión, se informó que si con posterioridad al envío de estas comunicaciones se hubiera procedido por las empresas

pertenecientes al Grupo a tratar los datos de aquellas personas que no se han opuesto a la cesión, dicho tratamiento podría ser denunciado a la Agencia.
Se terminó poniendo de manifiesto, al igual que en la consulta anterior, que la forma tácita de solicitar el consentimiento es lícita, siempre que no se trate de datos especialmente protegidos, correspondiendo a la Entidad que lo ha solicitado la prueba de que lo ha obtenido en cada caso concreto y señalando que dicho consentimiento tiene el carácter de revocable (art.11.4 LOPD)».

5.3 Tratamientos con fines históricos, estadísticos o científicos

El artículo 4.5 de la LOPD contiene una excepción conforme a la cual, atendiendo a los valores históricos, estadísticos o científicos de los datos y de acuerdo con la legislación específica aplicable en cada caso, puede decidirse el mantenimiento íntegro de determinados datos. Hablamos de un supuesto en el que no resulta necesario solicitar de nuevo el consentimiento pese a modificarse la finalidad para la que los datos fueron recogidos. Dicho artículo es desarrollado por el artículo 9 del Reglamento de desarrollo de la LOPD conforme al cual, para la determinación de los fines históricos, estadísticos o científicos se estará a la legislación aplicable, citando de forma expresa a :

- Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública.
- Ley 16/1985, de 25 junio, del Patrimonio histórico español.
- Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

Como excepción a la obligación de cancelación de los datos, la Agencia Española de Protección de Datos o, en su caso, sus homólogas autonómicas podrán, previa solicitud del responsable del tratamiento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas referidas anteriormente. Con este fin, el Reglamento de desarrollo de la LOPD establece un procedimiento, regulado en sus artículos 157 y 158, para la obtención de una declaración de la Agencia Española de Protección de Datos respecto a la concurrencia de los requisitos establecidos para el tratamiento de datos con valor histórico, científicos o estadísticos y que puede resumirse de la siguiente forma:

- Se iniciará siempre a petición del responsable que pretenda obtener la declaración.
- En el escrito de solicitud, el responsable deberá:

- Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.
- Motivar expresamente las causas que justificarían la declaración.
- Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

- La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.
- El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos.
- Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

6. Datos especialmente protegidos

Los artículos 7 y 8 de la LOPD establecen una serie de obligaciones relacionadas con el tratamiento de datos calificados como "*especialmente protegidos*". Se trata de un reforzamiento de las garantías entorno al tratamiento de estos datos considerándolos especialmente sensibles para la protección de los derechos y libertades de su titular. Nos encontramos en presencia de datos que aluden a la esfera más íntima del afectado y por tanto ha sido necesario establecer un régimen reforzado de protección.

Los artículos 7 y 8 de la LOPD son los siguientes:

«***Artículo 7. Datos especialmente protegidos.***

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan 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 precisará siempre el previo consentimiento del afectado.

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.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. 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 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 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.

*«**Artículo 8. Datos relativos a la salud.***
Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad».

6.1 Protección reforzada

Se encuentran fundamentos o antecedentes normativos concretos para esta protección en las siguientes normas:

- **Declaración Universal de los Derechos Humanos.** Su artículo 18, reconoce la libertad de pensamiento, de conciencia y de religión, ofreciéndole la libertad al individuo de ejercer esta libertad de manera pública o privada.

- **Constitución Española.**, Su artículo 16.2 dispone que "*nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*". De acuerdo con esto se aprecia la necesidad de establecer una mayor protección jurídica a este tipo de información personal.
- **Convenio 108 del Consejo de Europa.** Se ocupa de las "Categorías particulares de datos" y ofrece una enumeración cerrada de datos sensibles, indicando que «*los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales*[1]».
- **Directiva 95/46/CE.** Establece que, salvo que exista consentimiento del afectado, se haya hecho público por éste o exista otro bien jurídico protegido en juego, «*los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad*».

Por su parte la LOPD en su artículo 7 establece tres niveles de protección respecto a ciertos tipos de datos considerados sensibles distinguiéndose, por tanto: datos de carácter personal relativos a ideología, religión, creencias y afiliación sindical, datos personales relativos al origen racial o étnico, salud y vida sexual así como datos personales relativos a la comisión de infracciones penales o administrativas.

Por tanto, el régimen especial de protección establecido por la LODP se concreta en la necesidad de consentimiento expreso y por escrito del afectado para su tratamiento y en el establecimiento de una serie de prohibiciones o restricciones a dicho tratamiento, a saber:

- Consentimiento del afectado expreso y por escrito.
- Ciertas restricciones al tratamiento, limitándose al interés general o a una justificación legal en los casos en los que no sea el propio afectado quien expresamente consienta el tratamiento o cesión de sus datos personales.

6.2 Datos relativos a ideología, religión, creencias y afiliación sindical

6.2.1 Tratamientos comprendidos

Los relativos a la ideología, religión, creencias y afiliación sindical se encuentran regulados en los apartados primero y segundo del artículo 7 de la LOPD. En este sentido la Agencia Española de Protección de Datos, ateniéndose al principio de interpretación de los derechos fundamentales a favor de su titular, ha optado por una interpretación extensa de esta tipología de datos, de forma que en muchas ocasiones, y pese a que su tratamiento no afecte singularmente a la intimidad de la persona, se entiende que han de respetarse las previsiones de la normativa en materia de protección de datos de carácter personal. En este sentido es importante destacar que el artículo 7.2 de la LOPD alude a datos de carácter personal «*que revelen la ideología, afiliación sindical, religión y creencias*». Por tanto, la protección especial no se limita única y exclusivamente a los datos referidos a la ideología o religión, sino que son englobados en este concepto cualquier otro dato que pueda servir de indicio sobre estas características que se entienden dentro de la esfera más íntima de la personalidad. Dicha interpretación implica una serie de obligaciones para los responsables del tratamiento que en ocasiones pueden considerarse desproporcionadas en relación con el objeto y finalidad de dichos tratamientos.

Durante la vigencia de nuestra LOPD se han ido admitiendo supuestos en los que se ha dado una interpretación más flexible de esta obligación y así, la Agencia Española de Protección de Datos ha entendido que el dato de opción por la asignatura de religión no es un dato especialmente protegido, ya que:

«el hecho mismo de cursar la asignatura de religión no revela necesariamente que el estudiante profese las creencias a las que la asignatura se refiere, del mismo modo que el hecho de no cursarla no revela la inexistencia de esas creencias, sino que tal circunstancia puede deberse al estudio de la religión en otros foros distintos del escolar».

6.2.2 Consentimiento

Partimos de la regla general según la cual aquellos tratamientos que revelen ideología, afiliación sindical, religión y creencias solo podrán ser llevados a cabo cuando el interesado haya prestado consentimiento expreso y por escrito. En este caso, el responsable del tratamiento tiene la

obligación de advertir al interesado de su derecho a no prestar dicho consentimiento, de acuerdo con lo establecido por el artículo 16 de la Constitución Española: «*Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*»

Sin embargo dicha regla general no está libre de excepciones. En concreto la LOPD prevé dos excepciones a esta regla de consentimiento que en ningún caso eliminan la obligación del responsable del tratamiento de informar al interesado en los términos del artículo 5 de la LOPD:

- Ficheros mantenidos por partidos políticos, sindicatos, iglesias, confesiones, comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical. Estas organizaciones podrán tratar los datos personales de sus asociados o miembros sin necesidad de recabar el consentimiento previo y por escrito.
- Los supuestos del artículo 7.6 de la LOPD: «*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 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*»

6.2.3 Excepciones

Tal y como establece el artículo 7.4 de la LOPD existe una prohibición general de tratar estos datos cuando dicho tratamiento se lleve a cabo con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión o creencias de su titular.

6.3 Datos relativos al origen racial o étnico, salud y vida sexual

Son regulados por el artículo 7.3 de la LOPD si bien, la Agencia Española de Protección de Datos tiende a una interpretación amplia del concepto: *"datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual"*.

6.3.1 Datos médicos

La LOPD no realiza una definición expresa del concepto de salud., No obstante, la Agencia Española de Protección de Datos se apoya en las normas contenidas en los Tratados Internacionales de Protección de Datos suscritos por España. En este sentido, podemos citar la Recomendación R (97)[107] del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos que nos ofrece una definición de este tipo de datos:

«La expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos»

La profesora Coudert[108] completa esta definición:

«Conforme a esto, entenderemos por "dato de salud", cualquier información relativa a la salud pasada, presente y futura, física o mental, de un individuo, incluyendo las informaciones relativas al abuso del alcohol o al consumo de drogas, así como las informaciones genéticas. En esta categoría cabe incluir los datos psicológicos, sean extraídos de expedientes médicos, de las propias manifestaciones de los sujetos encuestados o de la apreciación del encuestador ante las citadas afirmaciones».

107 Consejo de Europa (1997). Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos.

108 COUDERT, F. (2005) *Tratamiento de datos especialmente protegidos, Estudio práctico sobre la protección de datos de carácter personal*. Cristina Almuzara Almaida, (Coord.). Editorial Lex Nova. Valladolid. Página 307.

6.3.2 Tratamiento de datos de salud

El artículo 7.3 LOPD restringe los supuestos en los que se permite su tratamiento, estableciendo una doble habilitación conforme a la cual 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 en los siguientes supuestos:

- Cuando por razones de interés general, así lo disponga una ley. En este sentido, no se establece ningún requisito adicional, más allá del necesario rango de Ley que deberá tener la norma que habilite la recogida de los datos.
- Cuando el afectado consienta expresamente. La LOPD no exige que este consentimiento expreso sea prestado por escrito, aunque en el momento de la recogida el responsable del tratamiento deberá asegurarse de que el interesado consiente de forma expresa al tratamiento de sus datos.

Cabría añadir la previsión del artículo 7.6 de la LOPD que también resulta de aplicación a los datos de salud, constituyendo una excepción al régimen establecido por el artículo 7.3de la LOPD:

- Los datos de salud podrán ser tratados cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

Conviene también hacer una mención a los supuestos de cesión de estos datos en base a lo establecido en el artículo 10.5 del Reglamento de desarrollo de la LOPD:

«Supuestos que legitiman el tratamiento o cesión de los datos: (…)
5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre. En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud 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».

6.3.3.Datos relativos a la comisión de infracciones penales o administrativas

El artículo 7.5 de la LOPD, establece en relación a los tratamientos de datos personales relativos a la comisión de infracciones penales o administrativas que estos sólo puedan ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. Dicho establecimiento comprende a todos los datos que revelen la comisión de infracciones sancionadas por la jurisdicción penal o las autoridades administrativas. En este sentido el profesor Rebollo comenta al hilo de una Sentencia de la Audiencia Nacional[109]:

«Resumimos en primer lugar, los Antecedentes de Hecho:

- *La Agencia Española de Protección de Datos, recibe denuncia de la Dirección General de la Policía, en la que se informa que vía Internet y en nombre la Asociación contra la tortura, se ofrecía un listado de datos sobre policías, guardias civiles y políticos, supuestamente implicados en actuaciones relativas a torturas.*
- *En lo publicado en Internet consta: listado con nombre de los funcionarios, su situación en relación con la denuncia por tortura (se está investigando, condenado, absuelto), el lugar de los hechos, la fecha, y la identificación del caso.*
- *La Agencia realiza las investigaciones pertinentes, y encuentra en la sede de la citada Asociación un servidor web, donde se publican datos relativos a 1994, 1995, 1996 y 1997, de las características mencionadas en el apartado primero.*
- *La Agencia Española de Protección de Datos adoptó la medida cautelar de cesar de forma inmediata el tratamiento de los datos y su difusión por vía de Internet, e inicia el expediente sancionador, que culmina con la imposición de las siguientes sanciones:*
  - *Por infracción de los artículos 6.1 y 7.5 de la LO 15/1999, 10.000.000 de pesetas.*
  - *Por infracción del art. 11 de la LO 15/1999, 50.000.000 de pesetas.*
- *La resolución de la Agencia es recurrida en reposición, siendo desestimado el recurso en resolución de 3 de octubre de 2000, por lo que se inicia el correspondiente recurso contencioso-administrativo ante la Audiencia Nacional, que dicta sentencia de fecha 28-2-2003, y cuyos contenidos jurídicos desglosamos en el siguiente apartado.*

109 REBOLLO DELGADO, L. (2004) *Difusión a través de Internet de infracciones penales o administrativas, sin consentimiento de los interesados.* Revista Datos Personales, Número 9, Mayo de 2004.

Ante estos hechos, la Audiencia Nacional entró a analizar las alegaciones de la Asociación, de las que destacamos, en relación a la restricción al tratamiento que estamos analizando, la afirmación de que los datos que poseía dicha Asociación, no tienen el carácter de datos personales, y que pueden ser revelados en virtud al derecho de libre expresión e información.»

En el análisis del profesor Rebollo se incluye la respuesta de la Audiencia Nacional sobre esta cuestión:

"En tercer lugar, la Asociación recurrente, sostiene que los datos recogidos en el fichero no son datos de carácter personal, pues los mismos no forman parte de la intimidad del individuo, y están supeditados al derecho de libertad de expresión e información, debido a que son personas que desempeñan una función pública, y por lo tanto, pueden ser objeto de tratamiento.

A juicio de la Audiencia, es jurisprudencia sentada por el Tribunal Constitucional en STC 292/2000, que la protección alcanza no sólo a los datos privados o íntimos, sino también 'a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos'.

También recuerda la sentencia, y a nuestro juicio, esta la parte de la construcción jurídica más significativa, la diferenciación entre 'dato personal' y datos de carácter personal'. Así, 'los primeros hacen referencia a cualquier información existencial ' vg: nacimiento, muerte, condena penal, etc... Para que los datos personales se conviertan en datos de carácter personal es preciso que permitan su conexión con relación a una persona concreta, determinada o determinable'.

Continúa manifestando la sentencia, que 'aplicando lo anterior al caso de autos, es claro que en contra de lo que se sostiene sí estamos ante un dato de 'carácter personal', pues en el listado se da una información ' la existencia de una denuncia por torturas y su situación ' puesta en conexión con el nombre y apellidos del denunciado, sin que la condición de cargo o funcionario público implique una exclusión constitutiva del carácter de dato personal, que como hemos visto se refiere en palabras del propio Tribunal Constitucional, no sólo a los datos íntimos, sino también a los públicos.

A continuación, la Audiencia referencia el contenido del art. 7.5 de la LO 15/1999, en relación a los datos relativos a infracciones penales o administrativas, que solo podrán ser incluidos en ficheros

de las Administraciones competentes, por lo que a su juicio esta prohibición está vigente, independientemente del origen público o privado del dato. Además, como acredita la Audiencia 'no todos los datos se extraen de sentencias, noticias de periódicos y denuncias de las que tiene conocimiento por su intervención como Asociación', ya que 'se recogen supuestos procesales no concluidos por sentencia y en tramitación'.

De todo lo manifestado, concluye la sentencia, que la Asociación 'ha infringido con nitidez lo establecido en el artículo 6.1 y 7.5 de la LO 15/1999, al tratar datos sin el consentimiento de los afectados y cuyo tratamiento se encuentra expresamente prohibido por la ley'. Además de lo manifestado, se estima probado 'que ha procedido a la cesión de tales datos con infracción nítida de lo establecido en el art. 11 de la LO 15/1999.»

6.4 Historial clínico

El tercer apartado del artículo 7 de la LOPD establece que los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente . Por tanto en esta caso, el tratamiento de datos relativos a la salud no precisará consentimiento por escrito, sino únicamente expreso por el interesado y en su caso habilitación legal. Además, estos datos podrán ser objeto de tratamiento, cuando dicho tratamiento 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 podrán tratarse dichos datos en los casos en los que 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.

Nos encontramos, por tanto, en presencia de una habilitación especial, necesaria para que los profesionales y organizaciones mencionados puedan llevar a cabo la prestación de sus servicios y un supuesto en el que la Agencia Española de Protección de Datos ha abogado también por una interpretación restrictiva. Conforme a la habilitación contenida en el artículo 8 de la LOPD, las Comunidades Autónomas con competencias en el ámbito de la salud han ido adoptando normas al respecto, dándose ciertas disparidades legislativas. La aprobación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia

de información y documentación clínica ha significado el necesario grado de uniformidad en esta materia. La norma incluye la regulación de aspectos directamente relacionados con la protección de los datos que los pacientes entregan en el marco del tratamiento médico al que son sometidos. Tal y como recoge la Exposición de motivos de la Ley 41/2002:

«(…) mantiene el máximo respeto a la dignidad de la persona y a la libertad individual, de un lado, y, del otro, declara que la organización sanitaria debe permitir garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación».

6.4.1 La historia

Tal y como establece el artículo 14.1 de la Ley 41/2002, 1. La historia clínica es el conjunto de todos los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

En este sentido, la finalidad principal de este tratamiento consistirá en facilitar la asistencia sanitaria dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud del paciente. La presente disposición se completa con lo establecido en el artículo 4 de la Ley 41/2002 que recoge el derecho a la información asistencial:

***«Artículo 4. Derecho a la información asistencial**.*
1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias.
2. La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar

decisiones de acuerdo con su propia y libre voluntad.
3. El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle».

Su interpretación conjunta permite definir con precisión qué datos pueden incorporarse para cumplir con la obligación prevista en el artículo 4.2 de la LOPD que como sabemos impide el uso de los datos para finalidades incompatibles. En cuanto al responsable del tratamiento, tendrá esta consideración el centro sanitario en el que se lleve a cabo el tratamiento médico o, en su caso, el profesional sanitario que ejerza de forma individual. Todo esto no excluye la obligación del profesional de colaborar a la adecuación de los datos de carácter personal tratados a lo exigido por la normativa tal y como se establece en la Ley 41/2002:

«Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes.
La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.
Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen».

6.4.2 Tratamiento de historiales clínicos

Se deberán tener en cuenta los siguientes aspectos:

- Principio de información. Pese a que la Ley 41/2002 no indica nada al respecto, no debemos olvidar que este tipo de tratamiento requiere cumplir con el principio de información establecido en el artículo 5 de la LOPD.
- Conservación de los datos. En lo que se refiere al principio de calidad, y en concreto a la conservación de los datos, el artículo 17 de la Ley 41/2002 establece: «*1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no*

necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

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

3. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal».

- Personas autorizadas a acceder a los datos personales. La historia clínica es un instrumento destinado a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales accederán a la misma en función de lo dispuesto por el artículo 16 de la Ley 41/2002 que dispone:

  «***Artículo 16. Usos de la historia clínica.***

  1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

  2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

  3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan 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 los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los

fines específicos de cada caso».

Observamos que la normativa impone un acceso restringido a este tipo información, de forma que el personal de administración y gestión de los centros sanitarios sólo podrá acceder a los datos de la historia clínica relacionada con sus propias funciones. Adicionalmente, el punto tercero de este artículo prevé el acceso a esta información con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia que se regirán por lo dispuesto en la LOPD. Ante esta habilitación, y como señala Herrán Ortiz[110] cabe preguntarse si únicamente para el acceso a la historia clínica con estos fines será de aplicación lo dispuesto en la LOPD.

7. Seguridad

Mientras que para el resto de principios es necesaria la obligación de respetar una serie de normas o criterios en el tratamiento de datos, el principio de seguridad exige una actitud más activa del responsable del tratamiento, obligado a implantar las medidas necesarias para garantizar la seguridad del tratamiento. Por tanto, el cumplimiento del principio de seguridad constituye la principal fuente de obligaciones y porqué no decir, también de costes que debe afrontar el responsable. Como antecedentes podemos citar el artículo 7 del Convenio 108 del Consejo de Europa así como el 17 de la Directiva 95/46/CE.

En concreto el primer apartado del artículo 17 de la Directiva establece:

"***Artículo 17. Seguridad del tratamiento***

1. *Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.*

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse»

110 HERRAN ORTIZ, A. (2003), *La protección de datos sanitarios. Especial referencia a la Ley 41/2002, de 14 de noviembre, reguladora de los derechos*. Revista de Derecho VLex, número 12, diciembre de 2003.

En este sentido podemos observar como el legislador europeo tuvo en cuenta los aspectos económicos siendo plenamente consciente del importante volumen de recursos que la aplicación del principio de seguridad puede suponer. Por contra, nuestro legislador, en la redacción del artículo 9 de la LOPD no tuvo en cuenta este aspecto:

*«**Artículo 9. Seguridad de los datos.***
1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán 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 estén expuestos, ya provengan de la acción humana o 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».

Por otro lado, la LOPD se refiere a medidas de índole técnica y organizativa, con lo que se abre el abanico de las medidas exigibles, ya que en última instancia es la vía reglamentaria la que decide las medidas de seguridad necesarias para garantizar el tratamiento de los datos personales de forma que se garantice, en todo caso, los derechos y libertades de los interesados.

Siguiendo a Martínez Sánchez[111] los objetivos del principio de seguridad son los siguientes:

- Crear un marco general, que facilite la elaboración e implantación de medidas técnicas y organizativas que garanticen un tratamiento adecuado de los datos personales.
- Sensibilizar y concienciar a los implicados en el tratamiento de datos personales, informando sobre los riesgos que implica su uso.
- Complementar las medidas de seguridad técnicas con medidas organizativas y de gestión, para alcanzar una seguridad material de los datos personales.
- Facilitar una clasificación de los ficheros y tratamientos de datos en atención a los riesgos

111 MARTÍNEZ SÁNCHEZ, M. (2000). *Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.* AJA, número 35.

que conlleven y a la naturaleza de los datos objeto de tratamiento.

- Exigir un nivel de seguridad adecuado, que favorezca el equilibrio entre los riesgos, los conocimientos técnicos existentes y el coste de aplicación de las medidas, para facilitar la evaluación continua de los sistemas de seguridad adoptados.

III. CONFIDENCIALIDAD Y DEBER DE SECRETO

1. Introducción

La confidencialidad y el deber de secreto se encuentran regulados en el artículo 10 de la LOPD:

«***Artículo 10. Deber de secreto.***
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estén 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».

Uno de sus principales objetivos es evitar que aquellas personas que están en contacto con los datos personales almacenados en ficheros, puedan vulnerar los derechos reconocidos, por la normativa, a sus titulares Sin embargo, al aludir al *secreto profesional* se produce cierta falta de concreción que es necesario aclarar en varios sentidos:

- Es preciso diferenciar de forma adecuada el deber de secreto, del secreto profesional.
- Aclarar la indefinición, expuesta por diversos autores, en torno a la aplicación de las obligaciones que se derivan del deber de secreto.

2. Secreto profesional

1.1 Confidencialidad y deber de secreto

Una cosa confidencial es aquella que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas. Su estrecha vinculación con el deber de secreto, nos hace observar su alta condición intersubjetiva y donde subyace la intención del legislador de diferenciar ambas. Por tanto, hablamos de confidencialidad cuando una persona que solicita algún tipo de servicio determinado realiza, de forma voluntaria, una reserva de sus datos más íntimos o de sus circunstancias personales, al entender que es preciso su conocimiento por el profesional para la prestación del

citado servicio. La confidencialidad consiste por lo tanto en una declaración de voluntad, mientras que el deber de secreto se configura como una obligación objetiva que le viene impuesta al facultativo por razón de su profesión. Debido a la ausencia en este caso del componente de voluntariedad que se aprecia en la confidencialidad, debemos entender que el secreto profesional supone el compromiso de la no divulgación de lo conocido en el ejercicio de la profesión.

En este sentido, cuando por razón de la actividad que se desempeña se llegan a conocer detalles referidos a la vida privada de otras personas existe un *pacto social* de que el profesional ha de guardar secreto respecto de tales hechos o detalles y el ordenamiento jurídico así lo reconoce desde distintos ámbitos: civil, administrativo y penal.

1.2 Fundamento del secreto profesional

Nuestra Constitución establece el secreto profesional en el artículo 20 y en el artículo 24.2. En lo relativo al derecho a la información el artículo 20 establece:

«La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades».

Mientras que en relación a la tutela judicial efectiva el artículo 24.2 dispone:

«La Ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos».

Existe por tanto, una estrecha relación entre el secreto profesional y el derecho a la intimidad. Esta interpretación ha sido acogida por nuestro Tribunal Constitucional al establecer que:

«El secreto profesional, en cuanto justifica, por razón de una actividad, la sustracción al conocimiento ajeno de datos o informaciones obtenidas que conciernen a la vida privada de las personas, está estrechamente relacionado con el derecho a la intimidad que el art. 18.1 de la Constitución garantiza, en su doble dimensión personal y familiar, como objeto de un derecho fundamental»

En este mismo sentido la Audiencia Provincial de Valencia en Sentencia de 4 de marzo de 2003

establece que:

«El secreto profesional del abogado impone al mismo, por razón de las particularidades propias de su actividad, la sustracción al conocimiento ajeno de cualesquiera datos o informaciones obtenidas por tal profesional que conciernan a las personas a las que se asesora o defiende, incluso el de la identidad de la persona a la que se imputa un delito o falta.

En tales casos, la observancia del secreto profesional protege un ámbito de reserva y sigilo en el ejercicio de una actividad profesional que, por su propia naturaleza o proyección social se estima merecedora de tutela. Esto se constituye en derecho obligación del abogado y, por supuesto, en derecho de su cliente merecedor de protección jurídica, y tan es así que la actuación contraria del letrado puede verse incluso penalmente sancionada.

Ciertamente, pueden plantearse algunos límites al derecho-deber de secreto profesional del abogado. No podría escudarse en el secreto profesional el abogado que, más allá de conocer datos o informaciones relativas a sus clientes, participara abiertamente en las actividades delictivas que pudieran llevar a cabo sus clientes, como autor o cómplice (arts. 27, 28 y 29 del Código Penal), ni tampoco podría pretender, amparándose en el secreto profesional, la impunidad de una actividad de encubrimiento típicamente descrita en el art. 451 del Código Penal. Igualmente, cabe pensar en algún supuesto hipotético en el que el principio de proporcionalidad y el estado de necesidad, permitieran transgredir la obligación del letrado de guardar secreto profesional, si mediante dicha transgresión se evitara la lesión de bienes jurídicos de superior valor, como pudiera ser la vida de una persona. Pero ninguno de estos casos se plantea en el supuesto de autos.

Además, la eventual exigencia de transgresión a un letrado de su secreto profesional, de proceder, debe regirse por un principio de subsidiariedad y última ratio, de forma que si el Juzgado que conoce de la denuncia de 30-11-98, puede obtener por otros medios la información que reclama, está obligado a acudir a ellos preferentemente. No es descabellado pensar que se pueda llegar a determinar la identidad de la persona buscada, sobre la base del conocimiento de los datos de que se dispone: se trata de un interesado en el cobro del mandamiento de devolución en el procedimiento de jura de cuentas 200/96, y, por lo que parece, familiar de la letrada. De no averiguarse, no obstante, no cabrá más que el sobreseimiento provisional de dicho procedimiento, sin poder deducir responsabilidad criminal del silencio de la letrada en esta causa por desobediencia, que deberá ser archivada y sobreseída libremente al amparo del art. 637-2 de la Ley de Enjuiciamiento Criminal».

En este punto es necesario ser cautos ya que el desarrollo legal al que alude el artículo 24.2 de la Constitución aún no se ha realizado y por tanto nuestra actual regulación del secreto profesional tiende a ser caótica. Por tanto, hasta que no se apruebe una ley en este sentido, la definición y aplicación de las obligaciones derivadas del secreto profesional, se encuentran recogidas por nuestro ordenamiento jurídico de forma muy dispersa y para sectores muy concretos y determinados.

1.2.1 Orden Administrativo

En el caso del **ámbito sanitario**, nos encontramos con la Ley 14/1986, de 25 de abril, General de Sanidad[2], así como con la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

El artículo 10 de la Ley 41/2002, alude al derecho de todos los ciudadanos al respeto de su personalidad, dignidad e intimidad en el ámbito de las diferentes Administraciones públicas sanitarias y, en el párrafo tercero, reconoce a todo usuario de la sanidad el derecho a *«la confidencialidad de toda la información relacionada con su proceso en instituciones sanitarias públicas y privadas que colaboren con el sistema público»*.

En relación al ejercicio de la abogacía debemos tener presente el Estatuto de la Abogacía fue aprobado por Real Decreto 2090/1982, de 24 de julio y establece el derecho y deber de guardar secreto profesional en relación con lo conocido por razón de su ejercicio, admitiendo que la tutela y defensa de intereses confiados al abogado, no puede justificar la desviación del fin supremo de justicia a que la Abogacía se halla vinculada.

1.2.2 Orden Civil

En este punto conviene destacar el artículo 1902 del Código Civil:

*«**Artículo 1902:** El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado»*

Se establece, en primer lugar, una obligación general para todo aquel que causa daño a otro, de

reparar el daño causado, con independencia de que exista culpa o negligencia. En base al citado artículo, el artículo 1903 dispone:

«***Artículo 1903:*** *La obligación que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder.*
Los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda.
Los tutores lo son de los perjuicios causados por los menores o incapacitados que están bajo su autoridad y habitan en su compañía.
Lo son igualmente los dueños o directores de un establecimiento y empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones.
Las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o extraescolares y complementarias.
La responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño».

Del contenido de este artículo se deduce que es aplicable en aquellos casos en los que la vulneración del deber de secreto se lleve a cabo por individuos que actúen bajo la responsabilidad de su empleador. En estos casos, corresponde al responsable del tratamiento probar que empleó toda la diligencia debida para la prevención del daño.

Para los casos de imputación de responsabilidad civil al responsable del tratamiento, el artículo 1904 del Código Civil ampara la posibilidad de iniciar las acciones necesarias para reclamar y resarcir el daño:

«***Artículo 1904:*** *El que paga el daño causado por sus dependientes puede repetir de éstos lo que hubiese satisfecho.*
Cuando se trate de Centros docentes de enseñanza no superior, sus titulares podrán exigir de los profesores las cantidades satisfechas, si hubiesen incurrido en dolo o culpa grave en el ejercicio de sus funciones que fuesen causa del daño».

1.2.3 Orden Penal

El Capítulo I del Título X del Código Penal versa sobre el *«descubrimiento y revelación de secretos»*. En concreto los artículos 197 y 199 establecen:

«***Artículo 197.***

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.»

«***Artículo 199.***

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

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

1.2.4 Orden Laboral

La exigencia del deber de secreto de los empleados se deriva directamente de lo dispuesto por los diferentes Convenios Colectivos así como por el Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. La obligación de secreto de los trabajadores en el desarrollo de las funciones para las que son contratados por el empleador se ampara en el deber de buena fe contractual.

En este sentido el artículo 5 del Estatuto de los Trabajadores consigna como uno de los deberes básicos de los empleados precisamente, el cumplir con las obligaciones concretas de sus puestos de trabajo, de conformidad a las reglas de la buena fe y diligencia. Por su parte, el artículo 54 del Estatuto recoge las causas del despido disciplinario y establece que el contrato de trabajo podrá extinguirse por decisión del empresario, mediante despido basado en un incumplimiento grave y culpable del trabajador, considerándose incumplimiento contractual, entre otros motivos, «*la transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo*».

Por otro lado es conveniente tener en cuenta el régimen de los funcionarios públicos en relación al incumplimiento del deber de secreto y, en concreto:

- El Real Decreto 33/1986, de 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado cuyo artículo 7.1.j) establece como falta grave: *«no guardar el debido sigilo respecto a los asuntos que se conozcan por razón del cargo, cuando causen perjuicio a la administración o se utilice en provecho propio»*.

- Los artículos 198 y 417 del Código Penal:
  «***Artículo 198.*** *La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.*
  «***Artículo 417.*** *1. La autoridad o funcionario público que revelare secretos o informaciones de los que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados, incurrirá en la pena de multa de doce a dieciocho meses e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años.*
  Si de la revelación a que se refiere el párrafo anterior resultara grave daño para la causa pública o para tercero, la pena será de prisión de uno a tres años, e inhabilitación especial para empleo o cargo público por tiempo de tres a cinco años.
  2. Si se tratara de secretos de un particular, las penas serán las de prisión de dos a cuatro años, multa de doce a dieciocho meses, y suspensión de empleo o cargo público por tiempo de uno a tres años».

1.3 Deontología

El deber de secreto profesional también se encuentra fundamentado por normas de tipo *ético-corporativas.* Por ejemplo, en el caso del ejercicio de la abogacía, el Consejo General de la Abogacía española, asumiendo lo dispuesto en el Código Deontológico Europeo, aprobó, el 30 de junio de 2000, el Código Deontológico.

Dicho Código establece en su artículo 5 el secreto profesional configurado como deber y derecho del abogado que no constituye sino concreción de los derechos fundamentales que el ordenamiento jurídico reconoce a sus propios clientes y a la defensa como mecanismo esencial del Estado de Derecho. Todo aquello que le sea revelado a un abogado por su cliente, con todas sus circunstancias, más todo aquello que le sea comunicado por otro abogado con carácter confidencial, deberá mantenerlo en secreto. No obstante, conviene recordar en este sentido la distancia existente entre los planos deontológico y jurídico. En el primer caso, hablamos de normas que afectan a aquellos profesionales sometidos a las mismas en función de su adscripción al Colegio Profesional. En el segundo, las pretensiones que frente a ellos se ejerciten por vulneración del deber de secreto deberán llevarse a cabo por vía judicial.

3. Deber de secreto

El artículo 16 de la Directiva 95/46/CE, establece:

«Las personas que actúen bajo la autoridad del responsable o encargado de tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal».

El presente artículo se limita a establecer la obligación de que el tratamiento se realice siempre bajo el encargo del responsable de tratamiento sin incorporar otras obligaciones o principios. Por otro lado, el artículo 10 de la LOPD llevó a cabo una regulación confusa de estas obligaciones, mezclando el contenido del artículo 16 de la Directiva con alusiones al deber de guardar secreto profesional respecto a los datos personales y que hemos tenido oportunidad de ver con anterioridad aunque llegados a este punto sea conveniente, matizar.

En primer lugar, recoge una doble obligación respecto a los datos a los que se acceda en cualquier fase del tratamiento: *«Deberá guardarse el secreto profesional y la debida confidencialidad»*. Por otra parte, es necesario insistir en el hecho de que el deber de secreto que establece la LOPD no es el secreto profesional.

Partiendo del deber de secreto profesional el artículo 10 LOPD alude al mismo para la definición del deber de secreto sobre los datos personales. De ello se deduce que no nos encontramos ante conceptos idénticos. Sin embargo parece que la intención del legislador ha sido trasponer las obligaciones que el ordenamiento jurídico preveía respecto al secreto profesional a todos aquellos que traten datos personales en el ejercicio de su actividad diaria. En este punto se debería tener en cuenta que la obligación contenida en el artículo 10 LOPD alude exclusivamente al ámbito administrativo y solo para lo que se refiere a los datos de carácter personal tratados así como que es necesario determinar, en base a la LOPD, quienes son los obligados por el deber de secreto y consecuentemente, sobre quien recaerán las consecuencias de su incumplimiento.

Parte de la doctrina se apoya en el contenido del artículo 7.6 de la LOPD para argumentar la diferencia entre ambos conceptos:

«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 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».

De esta alusión explícita de la LOPD al deber de secreto profesional cabe deducir que la exigencia del artículo 10 no alude al mismo concepto ya que decir lo contrario sería admitir la redundancia. De este argumento se deriva que el deber de secreto del artículo 10 de la LOPD no debe confundirse con el secreto profesional ya que se refiere a ámbitos distintos y está sujeto por un marco de responsabilidad propio,.

3.1 Ámbito objetivo

El principio de confidencialidad comporta que el responsable del tratamiento así como todas aquellas personas que intervengan en el mismo, no puedan revelar ni dar a conocer su contenido teniendo el deber de guardarlos. Este deber es una exigencia básica y comporta que los datos tratados no pueden ser conocidos por ninguna persona o Entidad ajena fuera de los casos autorizados por la Ley. El fin último del deber de secreto trata de garantizar el derecho de las personas a mantener el poder de control o disposición sobre sus datos.

3.2 Ámbito subjetivo

Aunque la LOPD sólo se refiere de forma expresa al responsable del tratamiento así como a todos aquellos que intervengan en cualquier fase, es evidente que esta obligación también incumbe directamente a los encargados del tratamiento y a quienes dentro de su organización, intervengan en cualquier fase del tratamiento de los datos. Para cada uno de ellos, la obligación de secreto así como el deber de guardarlos (respecto a los datos de carácter personal que conozcan y a los que tengan acceso en el ejercicio de sus funciones), subsistirá aún después de finalizar sus relaciones tanto con el responsable del tratamiento como con el encargado.

Por tanto, es necesario llevar la obligación de confidencialidad hasta aquellas personas que son las que realmente acceden a los datos personales en el ejercicio de su actividad, recayendo sobre el empleador la diligencia de velar porque esta obligación se cumpla, tanto si se encuentra en la posición jurídica de responsable como si lo hace en calidad de encargado.

4. Cumplimiento del deber secreto

Para cumplir con la obligación contenida en el artículo 10 de la LOPD, es conveniente:

- Identificar los activos de información y los accesos que a los mismos se realizan, tanto por nuestro personal como por colaboradores externos.
- Incluir en los contratos de trabajo cláusulas relativas al deber de secreto respecto de los datos personales a los que tengan acceso los empleados como consecuencia de su actividad.
- Extender esta obligación de confidencialidad a los empleados y colaboradores externos de las empresas prestatarias de servicios para la Entidad con acceso a los datos personales de los clientes.
- Elaborar políticas internas que garanticen la confidencialidad de la información, establecimiento los medios para su adecuada difusión y conocimiento por parte de todos aquellos que accedan a los datos personales gestionados por la organización.
- Llevar a cabo una revisión de las páginas web de acceso a los servicios que deben estar diseñadas de forma que no proporcionen al usuario más datos personales que los introducidos por el propio usuario, hasta que éste no haya superado con éxito los controles de identificación y autenticación.
- Proteger adecuadamente todos los soportes identificados (correo electrónico, documentación en papel, …)
- Regular contractualmente el acceso de datos por cuenta de terceros.

Una de las medidas más importantes es la elaboración y suscripción de acuerdos de confidencialidad. Si bien el secreto de los trabajadores se encuentra amparado en el Estatuto de los Trabajadores, en los términos expuestos anteriormente, es altamente recomendable, en todas las entidades que traten datos personales la firma de un acuerdo de confidencialidad entre la Entidad y sus empleados y colaboradores.

En relación a los aspectos que debe ser necesario considerar a la hora de redactar un acuerdo de estas características, conviene citar los siguientes[112]:

- Definir el ámbito temporal de la obligación.
- Especificar detalladamente la información, documentos, así como datos que serán considerados como confidenciales, siendo muy útil enumerarlos.
- Establecer la obligación de devolver a la Entidad contratante todas las copias o documentos, independientemente del soporte en el que se encuentren, relativa a la información a la que haya tenido acceso el trabajador como consecuencia del servicio prestado.
- Enumerar las excepciones en relación con aquellos documentos e informaciones que no se considerarán como confidenciales.
- Indicar expresamente la prohibición, salvo autorización previa, de comunicar dicha información a terceros.

112 NAVALPOTRO, Y. (2005). *El Deber de Secreto, Estudio Práctico sobre la protección de datos de carácter personal.* ALMUZARA ALMAIDA, C. (Coord.). Lex Nova. Valladolid.

IV. CESIÓN O COMUNICACIÓN DE DATOS

1. Introducción

La LOPD, define en su artículo 3, apartado i), la cesión o comunicación de datos como «*toda revelación de datos realizada a una persona distintas del interesado*». Sin embargo es una figura, que tiene una tremenda semejanza con el acceso de datos por cuenta de terceros y por ello la LOPD les dedica artículos distintos, el 11 para las cesiones o comunicaciones de datos y el 12 para el acceso de datos por cuenta de terceros o encargo del tratamiento.

Hemos de partir de la base de que ambas figuras son de extremada complejidad dada su gran variedad de supuestos y que la propia Agencia Española de Protección de Datos, destaca las cuestiones más controvertidas y que generan mayor número de conflictos, consultas y expedientes sancionadores. En todo caso es necesario tener presente que, cada caso concreto, sólo puede ser objeto de encaje en alguna de estas dos figuras y nunca, bajo ningún concepto una misma situación puede ser al mismo tiempo cesión de datos y encargo del tratamiento. Así se establece en la propia LOPD cuyo apartado primero del artículo 12 establece que *«no se considerará comunicación o cesión de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del fichero»*.

2. Cesión o comunicación de datos

Las cesiones o comunicaciones de datos, se encuentran reguladas en los artículos 11 y 27 de la LOPD. Como ya hemos visto la cesión o comunicación de datos supone *«toda revelación de datos realizada a persona distinta del interesado»*, esto es, de la persona física titular de los datos personales. Una definición demasiado amplia, quizá, y que abarca una gran cantidad de casuística tanto desde el punto de vista de los ficheros automatizados como desde el punto de vista de los no automatizados: entrega de soportes, consultas, interconexiones de ficheros, transferencias de datos, comunicaciones verbales y un largo etcétera.

El artículo 11 de la LOPD dispone:

«***Artículo 11. Comunicación de datos.***

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

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

a. Cuando la cesión está autorizada en una ley.

b. Cuando se trate de datos recogidos de fuentes accesibles al público.

c. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

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

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

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

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

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

2.1 Requisitos generales de la cesión o comunicación

La regla general, contenida en el artículo 11.1 LOPD dispone de tres requisitos básicos:

- Que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
- La necesidad de contar con el consentimiento previo del interesado.
- Obligación de informar a los afectados en el momento de la primera cesión.

En todo caso, el primer requisito que establece el artículo 11 LOPD para que la cesión pueda llevarse a cabo con garantía de cumplimiento del derecho a la protección de los datos de carácter personal es cumplir con el deber de información, contenido en el artículo 5 de la LOPD y que para el caso de las cesiones implica informar sobre la finalidad que justifica la cesión así como de la identidad de los destinatarios de la información.

Sobre la forma en la que se debe cumplir con esta obligación la Memoria de 1999[113] de la Agencia Española de Protección de Datos indica, en relación con una carta enviada a los abonados de una empresa del sector electrónico, en la que se solicitaba el consentimiento para comunicar los datos personales al resto de las empresas del grupo, que la información relativa a la finalidad que justificase la cesión debería ser explícita, determinada y legítima. Es decir, al titular de los datos no debe quedarle duda alguna acerca de cual es la finalidad a la que se destinarán sus datos.

En este mismo sentido, la Agencia señala[114]:

«La información al titular de los datos que vayan a ser objeto de cesión podrá referirse genéricamente a un sector de actividad, por ejemplo, servicios financieros), no admitiéndose finalidades indeterminadas o no comprensibles para el usuario (por ejemplo, actividad comercial, actividad publicitaria, empresas del grupo) (…)»

En todo caso, la Agencia Española de Protección de Datos recomienda la inclusión de la relación

113 Agencia Española de Protección de Datos. *Memoria del año 1999*, [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_1999/common/pdfs/MemoriaApd1999.pdf

114 Recomendaciones de la Agencia Española de Protección de Datos al Sector del Comercio Electrónico para la adecuación de su funcionamiento a la LOPD, publicada en la Memoria anual correspondiente al año 2000

completa de los datos relativos a todas las entidades cesionarias, en la medida en que sea posible para el responsable del fichero en el momento de la recogida.

2.1.1 Finalidades legítimas

La finalidad que justifica el tratamiento debe estar relacionada, de forma directa, con las funciones legítimas del cedente y del cesionario. Debemos entender por *funciones legítimas*, todas aquellas actividades amparadas por la Ley, excluyendo este concepto por lo tanto, la cesión de datos para el cumplimiento o desarrollo de funciones o actividades ilícitas, ilegales, constitutivas de delito, o análogas.

Sobre el requisito de que dichas funciones legítimas guarden relación directa con las actividades profesionales del cedente y del cesionario el legislador pretendió introducir un elemento adicional de control sobre las cesiones de datos, de forma que no fuera posible llevar a cabo cesiones ilimitadas amparadas en formas poco estrictas de recogida del consentimiento. Evidentemente esta condición no será aplicable en caso de que se recabe consentimiento expreso del interesado para la cesión, independientemente de que exista o no una relación directa entre los fines de la cesión y las funciones de las partes que intervienen en ella.

2.1.2 Obtención del consentimiento

Se deberán tener en cuenta dos posibilidades en relación a la obtención del consentimiento:

- **La cesión va a ser el único tratamiento a llevar a cabo por el Responsable del Tratamiento:** La finalidad de la cesión deberá ser informada en el momento de proceder a la recogida de los datos siendo necesario incluir la identificación del cesionario o cesionarios de los datos.
- **Si, adicionalmente a la cesión, se pretende llevar a cabo otro tipo de tratamiento:** La captación de datos se lleva a cabo para la realización de sus fines generales dentro de su ámbito de actividad y, adicionalmente, se tiene intención de ceder los datos personales a terceros.

En este punto es de vital importancia tener en cuenta que la capacidad de acreditar el consentimiento del titular para la cesión es uno de los puntos *vitales* a la hora de determinar la

existencia de un posible incumplimiento en esta materia. Será necesario solicitar al interesado el consentimiento para que autorice los tratamientos así como las cesiones o comunicaciones de datos. En cierto que bajo este sistema no se está ofreciendo al interesado la posibilidad de prestar su consentimiento sólo a algunas de las comunicaciones. Sin embargo la Agencia Española de Protección de Datos ha considerado válido este sistema ya que en todo caso el consentimiento aportado para las cesiones siempre tienen un carácter revocable, tal y como establece el artículo 11.4 de la LOPD.

Asimismo conviene recordar el artículo 11.3 de la LOPD: «*Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar*». Por tanto, siempre que la información facilitada al titular sea errónea, induzca a error o simplemente no sea explícita y determinada no permitiendo conocer con certeza la identidad del cesionario y la finalidad del tratamiento, el consentimiento será considerado nulo.

Además debemos tener en cuenta que el consentimiento puede ser tanto expreso como tácito, siendo este último tipo de consentimiento uno de los que mayores problemas plantea. En este sentido, la Audiencia Nacional en su sentencia de 7 de julio de 2000[115] establece:

«*(…) el tema del consentimiento tácito ha de ser tratado con gran delicadeza*
(…) este tema del consentimiento tácito ha de ser tratado con una gran delicadeza cuando están en juego derechos constitucionales básicos (art. 18.4 C.E.) y a ello tiende toda la regulación legal contenida en el articulado de la L.O. 5/92 y su explicación y filosofía recogida en la Exposición de Motivos.
En la vida de relación es muy posible reconocer formas de tácita aceptación, pero siembre en aspectos no trascendentales o cuando se está operando sobre situaciones consolidadas y que están en la común consideración a modo de valores entendidos. No es el caso cuando lo que está en juego es la privacidad de las personas de ahí todas las cautelas normativas tendentes a proteger esa privacidad, sin que quepan interpretaciones de laxitud del artículo 11.1 de la Ley a menos que el titular de la intimidad se haya situado voluntariamente en situación de abandono de la defensa de ese derecho, en cuyo caso sí podría hablarse de una forma de consentimiento tácito».

115 Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 7 Julio de 2000. Recurso 121/1999.

En idéntico sentido se pronuncia el Tribunal Superior de Justicia de Madrid[116]:

«Pese a que la prestación del consentimiento consciente e informado no parece mostrarse en el tráfico ordinario sino, por lo común, en su forma expresa, la hipotética admisión del consentimiento tácito, que es lo que propugna la recurrente, requeriría en todo caso su manifestación a través de actos concluyentes.
Pues bien, no hay acto alguno del titular de los datos que pueda identificarse con la prestación de su voluntad de ser incluido en un fichero con fines de publicidad. Del simple acto de remitir un cupón para participa en un sorteo sólo puede inferirse el deseo de participar en éste, pero nunca el de ser incluido en un fichero automatizado».

La Agencia Española de Protección de Datos, aún admitiendo la prestación de un consentimiento tácito, éste debe, en todo caso, cumplir los requisitos de la definición recogida en el artículo 3.h) de la LOPD para que el consentimiento pueda ser considerado conforme a derecho. En particular, el consentimiento debe ser informado, de modo que el afectado conozca la existencia del tratamiento de los datos y la finalidad de su recogida tal y como establece el artículo 5 de la LOPD.

Sobre este punto Carrasco Linares y Puente Serrano[117] establecen que *«en el supuesto de plantarse algún tipo de conflicto o litigo respeto del hecho de si se ha recabado o no el consentimiento -tácito- del interesado para la cesión o comunicación de sus datos, será el responsable del fichero el que tenga atribuida la carga de la prueba -en ocasiones, difícil de demostrar- pudiendo emplear para ello documentos o cualesquiera otros medios de prueba válidamente admitidos por la legislación procesal, con el fin de acreditar el cumplimiento de la obligación de recabar el consentimiento».*

2.1.3 Primeras cesiones y deber de información

Este punto se encuentra regulado en el artículo 27.1 LOPD:

«1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los

116 Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-administrativo, Sección 9ª, Sentencia de 30 de enero de 2003. Recurso 1856/1997.

117 CARRASCO LINARES, J. y PUENTE SERRANO, N (2004). *Las relaciones entre empresas, La Protección de Datos en la Gestión de Empresas*. Editorial Thompson Aranzadi. El Cano (Navarra). Página 158.

datos que han sido cedidos y el nombre y dirección del cesionario».

En este sentido, la comunicación del artículo 27 debe realizarse en el momento de la primera comunicación, por lo que no será exigible en el supuesto de que esta no se lleve a cabo. Se trata de un requisito que parece reiterativo, ya que el titular ha debido de ser informado con carácter previo tal y como hemos visto. No obstante, hay que tener en cuenta, en primer lugar, que se establece una serie de excepciones a esta obligación en el segundo punto del mismo artículo 27:

«2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c, d, e y 6 del artículo 11, ni cuando la cesión venga impuesta por ley».

Siendo necesario entender que se trata de una garantía adicional para el caso de que la recogida del consentimiento se haya llevado a cabo de forma tácita. El titular de los datos podrá conocer en este caso quién posee sus datos y el tratamiento que con los mismos se está llevando a cabo.

2.2 Excepciones

La LOPD establece una serie de excepciones que es necesario no sólo tener en cuenta sino también analizar.

2.2.1 Cuando no es necesario recabar el consentimiento

Tal y como establece el artículo 11.2 LOPD:

«El consentimiento exigido en el apartado anterior no será preciso:
a. Cuando la cesión está autorizada en una ley.
b. Cuando se trate de datos recogidos de fuentes accesibles al público.
c. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación

tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

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

Analicemos cada apartado en profundidad.

A. Cuando la cesión está autorizada en una ley

La LOPD prevé los casos en los que la obligación de recabar el consentimiento esté previsto en una ley. En el ordenamiento jurídico español es posible encontrar supuestos en los que se autoriza a no recabar el consentimiento o incluso, casos en los que la Ley obliga a que se lleve a cabo la cesión. En este punto nuestro Tribunal Supremo sigue la doctrina de que cuando nos encontramos ante la obligación de ceder los datos personales, la persona física o jurídica obligada a la cesión no podrá alegar la protección del derecho a la intimidad o a la protección de los datos de carácter personal para justificar el incumplimiento de su obligación. Así se puede apreciar en su Sentencia de 29 de septiembre de 2002[118]:

«(…) En efecto, la cobertura legal la suministra el artículo 154 de la Ley de la Propiedad Intelectual (Real Decreto Legislativo 1/96 de 12 de abril), que atribuye al Ministerio de Cultura la vigilancia sobre el cumplimiento por las entidades de Gestión como la actora, entre otras obligaciones, de la del reparto de los derechos recaudados entre los titulares de los mismos en los términos del artículo 149.

De modo que el párrafo 1 del citado artículo 154, L.P.I., para hacer eficaz tal función de vigilancia, expresamente faculta al Ministerio de Cultura para exigir de esas entidades cualquier tipo de información y ello que determina que esa regulación legal haga ceder el derecho al secreto que respecto de los datos personales informatizados establece el artículo 10 de la Ley Orgánica 5/92,

118 Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 7ª, Sentencia de 26 de septiembre de 2005. Recurso 4673/1999.

sobre tratamiento automatizado de datos, o el derecho a la confidencialidad del artículo 7º de la Ley O. 1/1982, sobre protección del honor, la intimidad y la propia imagen, citadas a efectos de legitimación, pues el artículo 11 de la Ley Orgánica citada en primer lugar, exime del consentimiento del afectado la cesión de datos que sea consecuencia de una previsión legal, y el artículo 8º.1 de la Ley Orgánica de protección al honor, no considera intromisiones ilegítimas las acordadas por Autoridad competente conforme a la Ley. Era, pues, una actividad necesaria para los fines o intereses a tutelar por la Administración actuante.

Así se desprende, también, de compromisos internacionales suscritos por España en la materia (cuyo valor interpretativo viene refrendado por el artículo 10.2 del Texto constitucional), y, en especial, del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (de 28 de enero de 1981, ratificado por España por Instrumento de 27 de enero de 1984), en cuanto impone a los Estados firmantes, principios específicos de actuación para la obtención de datos, que garanticen la legitimidad de éstos, la adecuación de la información recibida en atención a las finalidades con ella perseguidas (artículo 5); un especial refuerzo de la reserva de datos en materias especialmente conectadas con el derecho a la intimidad (artículo 6); y la no difusión de «datos de carácter personal» (artículo 7). Todo ello, con el añadido de que las eventuales excepciones que puedan imponerse por cada Estado en las materias y ámbitos autorizados en el artículo 9 del convenio sean única y exclusivamente las necesarias «en una sociedad democrática».

En todo caso, la habilitación a la que se hace referencia de forma constante debe tener siempre rango de Ley, tal y como establece de forma expresa la propia LOPD.

B. Cuando se trate de datos recogidos de fuentes accesibles al público

Excepción regulada en el artículo 11.2 LOPD. En este punto es necesario tener en cuenta que el hecho de que no sea necesario recabar consentimiento en estos casos, no afecta a la necesidad de cumplir con el deber de información al titular de los datos personales, en los términos del artículo 5 de la LOPD, salvo que estos datos vayan a ser destinados a la actividad de publicidad o prospección comercial, en cuyo caso se deberán tener en cuenta los 5.5. y 30.2 LOPD. En todo caso, el cumplimiento de este deber de información no tiene porqué ser previo a la recogida de los datos, sino que podrá ser cumplido dentro del plazo de tres meses a contar desde que fueron recogidos o en el momento en el que tenga lugar el envío de cada comunicación al interesado.

Para Carrasco Linares y Puente Serrano[119] si debe ser cumplido el deber de información posterior a la primera cesión del 27.1 LOPD lo cual podría tener lugar incluso con anterioridad al cumplimiento del deber de información de los artículo 5.4 LOPD o 5.5 LOPD, siempre que la cesión tenga lugar antes de que haya sido enviada comunicación alguna al interesado, respectivamente.

C. Cesión como consecuencia de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros

Ante la falta de concreción de esta excepción ha sido necesario que la Agencia Española de Protección de Datos se pronuncie al respecto. En este sentido, uno de sus Informes[120], relativo a la posibilidad de ceder datos de compradores al productor de un producto, dispone:

«La consulta plantea si resulta conforme a la LOPD la comunicación a la empresa productora de un determinado producto de los datos identificativos de quienes adquirieron el mismo a través de la consultante, a fin de que la productora se ponga en contacto con aquéllos y retire los artículos adquiridos, al haberse detectado en los mismos un fallo en sus condiciones de estanqueidad que pudiera provocar daños en las personas.

La transmisión así planteada implica la existencia de una cesión o comunicación de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica 15/1999 como "Toda revelación de datos realizada a una persona distinta del interesado".

En relación con las cesiones, el artículo 11.1 de la Ley indica que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". No obstante, este consentimiento no será preciso, según el artículo 11.2 a), cuando una norma con rango de Ley otorgue cobertura a la comunicación. Del mismo modo, conforme al artículo 11.2 c) la cesión será posible sin contar con el citado consentimiento "cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con

119 CARRASCO LINARES, J. y PUENTE SERRANO, N (2004). *Las relaciones entre empresas, La Protección de Datos en la Gestión de Empresas*. Editorial Thompson Aranzadi. El Cano (Navarra). Página 166.

120 Agencia Española de Protección de Datos (2007). Informe 0055/2007 [en línea]. Comunicación de datos de compradores. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2007-0055_Comunicaci-oo-n-de-datos-de-compradores..pdf [2010, 16 de junio]

ficheros de terceros", si bien, "en este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique".

Tal y como se describe a lo largo de la consulta, la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, establece una serie de derechos de los consumidores, así como las correlativas obligaciones impuestas a los productores y distribuidores de los bienes adquiridos.

De este modo, como se indica en la citada consulta, el artículo 5.2 g) de la Ley impone al fabricante la obligación "de retirar o suspender, mediante procedimientos eficaces, cualquier producto o servicio que no se ajuste a las condiciones y requisitos exigidos o que, por cualquier otra causa, suponga un riesgo previsible para la salud o seguridad de las personas", habida cuenta que el artículo 2.1 a) reconoce el derecho del consumidos a la protección "contra los riesgos que puedan afectar a su salud o su seguridad". Igualmente, el artículo 25 añade que "El consumidor y el usuario tienen derecho a ser indemnizados por los daños y perjuicios demostrados que el consumo de bienes o la utilización de productos o servicios les irroguen salvo que aquellos daños y perjuicios estén causados por su culpa exclusiva o por la de las personas de las que deba responder civilmente".

Como también se indica en la consulta, la Ley 26/1984 se encuentra actualmente desarrollada, en lo que a la prevención de la seguridad en el consumo se refiere, por el Real Decreto 1801/2003, de 26 de diciembre, de Seguridad general de los productos.

El artículo 4.3 b) del citado Real Decreto dispone que "dentro de los límites de sus respectivas actividades y en función de las características de los productos, los productores deberán (...) cuando descubran o tengan indicios suficientes de que han puesto en el mercado productos que presentan para el consumidor riesgos incompatibles con el deber general de seguridad, adoptar, sin necesidad de requerimiento de los órganos administrativos competentes, las medidas adecuadas para evitar los riesgos, incluyendo informar a los consumidores mediante, en su caso, la publicación de avisos especiales, retirar los productos del mercado o recuperarlos de los consumidores".

A su vez, el Real Decreto impone una serie de obligaciones de comunicación a las autoridades administrativas de la existencia de la situación de riesgo mencionada.

Por su parte, el artículo 5.3 añade que "dentro de los límites de sus actividades respectivas, participarán en la vigilancia de la seguridad de los productos puestos en el mercado, en concreto (...) colaborando eficazmente en las actuaciones emprendidas por los productores y los órganos administrativos competentes para evitar dichos riesgos".

Según se indica en la consulta, se han adoptado las medidas de publicidad precisas para dar a conocer la existencia del defecto en el producto al que se refiere la consulta que puede dar lugar a la producción de daños en las personas, habiéndose producido la retirada del mercado de los productos defectuosos. No obstante, a fin de poder proceder a la retirada de los productos ya adquiridos, se solicitan del productor al distribuidor consultante los datos relativos a los adquirentes del citado producto.

La adquisición del producto da lugar al nacimiento de una relación jurídica entre el consumidor y el distribuidor de aquél sometida a las normas que garantizan la seguridad y, en su caso, integridad del consumidor y que aparecen reguladas por las normas que se han venido reproduciendo.

Si bien el productor no es parte directa en la citada relación si puede aparecer obligado por la misma, bien mediante la constitución de la garantía legalmente exigible, bien mediante el obligado cumplimiento de los requisitos legalmente exigibles para garantizar la mencionada seguridad del consumidor. Precisamente por ese motivo, el Real Decreto 1801/2003 viene a imponer al productor una serie de obligaciones que permitan garantizar, en caso de existir un riesgo para la seguridad del consumidor, la retirada del producto no sólo en el mercado, sino incluso en relación con aquellos que ya hubieran sido adquiridos.

En consecuencia, la relación derivada de la adquisición del producto no se extingue como consecuencia de la adquisición, existiendo una serie de deberes legales que deberán cumplirse con posterioridad al citado momento, garantizándose un adecuado seguimiento o control de la citada relación jurídica.

Ello implica que cuando los citados deberes incluyen la exigencia de proceder a la retirada del producto adquirido como consecuencia de la detección de riesgos graves para sus adquirentes el productor o fabricante deba no sólo dar a conocer la existencia de dichos riesgos, permitiendo así una conducta activa del consumidor que mediante la devolución eluda la producción del riesgo, sino igualmente deba adoptar las medidas que resulten necesarias para garantizar la recuperación

del producto del consumidor que lo adquirió.

De este modo, si el productor tuviera conocimiento de los datos de los adquirentes deberá adoptar las medidas necesarias para garantizar la retirada. Igualmente, de las obligaciones impuestas al mismo se desprende que deberá adoptar todas las medidas que diligentemente le permitan identificar al adquirente para llevar a cabo la retirada del producto.

Al propio tiempo, el distribuidor deberá adoptar las medidas necesarias para colaborar con el productor en la disminución del riesgo potencial que pudiera causar el producto por él comercializado.

De este modo, sin entrar a analizar si la cesión planteada podría encontrar efectivamente cobertura en las habilitaciones legales derivadas del tenor de la Ley 26/1984 no cabe duda que la comunicación por el distribuidor al productor de los datos de los consumidores finales de los que tenga conocimiento ha de considerarse necesaria para el adecuado mantenimiento, seguimiento y control de la relación jurídica generada como consecuencia de la adquisición del producto defectuoso.

Por ello, la cesión se encuentra amparada por el artículo 11.2 c) de la Ley Orgánica 15/1999, no siendo en consecuencia contraria a la misma y no incurriéndose en ningún tipo de infracción como consecuencia de la cesión».

D. Cesión al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas

En este punto debemos tener en cuenta que esta excepción tiene carácter de *numerus clausus* y por lo tanto, la excepción sólo es aplicable a los organismos citados en la misma y no es posible su aplicación por analogía.

2.2.2 Cuando no es necesario informar, de una forma posterior a la primera cesión

Nos encontramos en presencia de los supuestos establecidos en el artículo 27.2 de la LOPD y que versan sobre las siguientes cesiones:

- Cesión impuesta por una Ley.
- Cesión como consecuencia de la aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
- Cesión que tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales y el Tribunal de Cuentas.
- Cesión que tenga lugar entre Administraciones Públicas, siempre que se realice con la finalidad histórica, científica o estadística.
- Cesión efectuada previo procedimiento de disociación de los datos.

En todos estos casos, no será necesario recabar el consentimiento del titular así como informar con posterioridad.

Para finalizar el análisis de las cesiones o comunicaciones de datos únicamente nos queda referirnos a la figura del cesionario que, tal y como establece el artículo 11.5 de la LOPD queda obligado al cumplimiento de la normativa en materia de protección de datos de carácter personal:

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

3. Encargos del tratamiento

Tal y como establece la LOPD, el acceso a datos por cuenta de terceros se lleva a cabo por el encargado del tratamiento que es, tal y como establece el artículo 5.1 i):

«La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio».

La realidad de la externalización de servicios u outsourcing genera que hoy en día esta práctica sea habitual y cotidiana. En este sentido el artículo 12 LOPD dispone:

«***Artículo 12. Acceso a los datos por cuenta de terceros.***

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

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

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

Dicho artículo debe ponerse en relación con los artículos 20, 21 y 22 del Reglamento de Desarrollo de la LOPD:

«***Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.***

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el

establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.
No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. Posibilidad de subcontratación de los servicios.
1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a. Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b. Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c. Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los

términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. Conservación de los datos por el encargado del tratamiento.

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

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento».

3.1 El encargo del tratamiento en la Directiva 95/46/CE

La prestación de servicios a una Entidad (pública o privada) supone en la mayor parte de las ocasiones el tratamiento de los datos de carácter personal generados por el receptor del servicio durante el desarrollo de su actividad.

La Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos, vino a regular esta figura denominando "**encargado del tratamiento**" al prestador de servicios que accede a datos de carácter personal incluidos en los ficheros del responsable.

La definición que figura en su artículo 2, apartado e), y se repite de forma literal en la LOPD.

Asimismo el texto comunitario ubica las prescripciones relativas al encargado del tratamiento en los apartados 2 y 3 de su artículo 17, referido a la seguridad. De todo ello es posible deducir que la inclusión de esta figura obedece a la necesidad de regular el fenómeno de la externalización de los servicios, para que, en el supuesto de que se produzca un acceso a datos como consecuencia del mismo, se garanticen las medidas de seguridad apropiadas.

En este sentido, Heredero Higueras señala:[121]

«Este artículo es el resultado de la supresión del que en la propuesta de 1992 figuraba como artículo 24 y la consiguiente inclusión de sus disposiciones en un nuevo artículo 17 (primeramente 17 bis), del cual fue, a su vez, segregado el actual artículo 16. En realidad, este precepto trata dos temas independientes, por lo cual podría haber sido mantenido en la forma en que figuraba en el texto de 1992, o bien podía haber sido escindido en dos en función de las materias respectivas. Los apartados 1 y 2 tratan de las obligaciones del responsable del tratamiento en cuanto a medidas de seguridad de los datos, y los apartados 3 y 4 del tratamiento de datos efectuado por un encargado, según este concepto se define en el artículo 2,e). La inclusión de los temas en un mismo precepto se explica, sin duda, por la preocupación por la seguridad de los datos en los casos en que el proceso de los datos sale del control inmediato del responsable del tratamiento. Por eso, el apartado tres constituye un eslabón de enlace entre ambas cuestiones (….)».

En concreto, se determinan las siguientes garantías:

- El responsable del fichero deberá elegir un encargado del tratamiento que reúna garantías suficientes de cumplimiento de las medidas de seguridad técnicas y organizativas.
- La realización del tratamiento deberá estar regulada por contrato u otro acto jurídico en el que se especifique que:
  - El encargado del tratamiento sigue instrucciones del responsable del mismo.
  - El encargado del tratamiento debe cumplir las obligaciones en materia de seguridad que determine la normativa aplicable.

La figura del encargado del tratamiento se introduce en la LOPD como consecuencia de la transposición de la Directiva a nuestro ordenamiento. Constituye una de las novedades más

121 HEREDERO HIGUERAS, M. (1997). *La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.* Editorial Aranzadi. Elcano (Navarra). Páginas 162-164.

importantes de la LOPD con respecto a su predecesora, la LORTAD, que si bien, incluía una figura similar en su artículo *27: Prestación de servicios de tratamiento automatizado de datos de carácter personal*. El contenido de este artículo era mucho más limitado que el del actual artículo 12 de la LOPD, pues sólo se aplicaba al supuesto en el que el servicio que une a las dos empresas tuviera como objeto principal el tratamiento automatizado de datos. El encargado del tratamiento de la LOPD sin embargo, incluye cualquier prestación de servicios que requiera tratar datos del responsable del fichero de forma accesoria al objeto del contrato.

3.2 Características del encargo del Tratamiento

El legislador marca la diferencia entre ambas figuras, dejando claro que el tratamiento de datos por encargo no queda incluido dentro del régimen de la cesión de datos regulando por ello, estas figuras en distintos artículos.

Por tanto, el tratamiento de datos que sea necesario para la prestación de un servicio no tiene la consideración de comunicación y no aparece sometido a las reglas y excepciones dispuestas por el artículo 11 de la LOPD. El tratamiento de datos por encargo no es un supuesto de cesión de datos en el que el consentimiento esté exceptuado, sino una figura distinta a la cesión. A diferencia de la cesión o comunicación, el tratamiento de datos por encargo no precisa del consentimiento del interesado.

Sin embargo, para que opere el régimen del artículo 12, se exige como requisito la formalización de un contrato entre el responsable del fichero y el encargado del tratamiento con el siguiente contenido:

- El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- El encargado del tratamiento aplicará o utilizará los datos con fin distinto al que figure en dicho contrato.
- El encargado del tratamiento no comunicará, ni siquiera para su conservación a terceras personas.
- El encargado del tratamiento estará obligado a implementar las medidas de seguridad a que se refiere el artículo 9 de la LOPD.
- El encargado del tratamiento no podrá conservar los datos finalizada la prestación del

servicio.

El citado contrato debe constar por escrito o por cualquier otro medio que permita acreditar su celebración y contenido. Esto no significa que las partes deban firmar un contrato cuyo objeto sea regular el tratamiento de datos por cuenta de terceros, sino que podrá incluirse un anexo o una cláusula sobre este particular en el contrato de prestación de servicios. Ahora bien, el artículo 12 resulta de aplicación en un supuesto concreto en el que entre las partes existe una relación contractual de arrendamiento de servicios.

En este sentido, Aparicio Salom[122] indica:

«La relación contractual que se contempla en el artículo 12 de la LOPD es la de un arrendamiento de servicios, esto es, aquel contrato por el que una persona se compromete a prestar algún servicio a otra a cambio de un precio.
La característica esencial del contrato de arrendamiento de servicios es que quien los presta actúa por cuenta de quien lo encarga, de modo que el riesgo o beneficio de los resultados del servicio siempre recaerá sobre el arrendatario, esto es, quien encarga el servicio.
A su vez el arrendamiento de servicios puede pactarse de modo que el prestador del servicio actúe libremente, en atención sólo a la consecución de un resultado o conforme a las instrucciones de quien lo encarga, o, de forma mixta, con arreglo a las instrucciones del arrendatario y aplicando su leal saber y entender para la mejor consecución del resultado pretendido en cuanto al resto».

Nuestro derecho no obliga a que el contrato de arrendamiento de servicios se formalice por escrito. Por lo tanto, en caso de que la relación que una a las partes sea un acuerdo verbal, sí que deberá existir un contrato escrito específico que recoja lo previsto en el artículo 12. Por lo demás, existe un amplio marco de libertad para las partes en este supuesto de tal forma que el artículo 20 del Reglamento de desarrollo de la LOPD destaca este hecho afirmando que el servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

3.2.1 Tratamiento de los datos según las instrucciones del responsable

El encargado de tratamiento queda obligado, a tratar los datos conforme a las instrucciones del

122 APARICIO SALOM, J. (2000). *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal.* Editorial Aranzadi. Elcano (Navarra). Páginas 128 y 129

responsable del fichero, y al cumplimiento de los fines que expresamente hayan sido identificados en el contrato. Es posible que la finalidad de los tratamientos llevados a cabo por el encargado de tratamiento no coincida plenamente con las finalidades con la que fueron recogidos los datos por parte del responsable de tratamiento. Por ello, es conveniente regular con el mayor nivel de detalle posible dichas finalidades en el contrato que se formalice entre ambas partes.

3.2.2 Subcontratación

En este punto debemos citar el informe de la Agencia Española de Protección de Datos 582/2004[123] sobre subcontratación de servicios por el encargado del tratamiento:

«deriva directamente de la propia naturaleza del derecho fundamental a la protección de datos de carácter personal.
En este sentido, si dicho derecho consiste, según indica el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, en un poder de disposición del afectado sobre la información que le concierne, resulta lógico que, habiendo autorizado (o habiendo previsto la Ley) que los datos puedan ser objeto de tratamiento por parte de un determinado responsable, será preciso que dicho responsable conozca en cada momento que terceras entidades acceden a dichos datos, siempre en su nombre, a fin de garantizar al interesado que los datos de los que el mismo es titular no excedan del control de aquella Entidad cuyo tratamiento ha sido aceptado por aquél».

El supuesto que estamos analizando afecta por lo tanto a la posibilidad de subcontratación por parte del encargado de tratamiento con terceros que puedan prestar algún servicio. En este informe la Agencia matiza la prohibición del artículo 12, permitiendo la subcontratación si el responsable del fichero la conoce o la autoriza, con su participación en un contrato con el subcontratista o bien encomendando un apoderamiento al encargado del tratamiento. No obstante, hasta la publicación del Reglamento de desarrollo de la LOPD, el tema de la subcontratación no fue resuelto completamente.

Si bien, la Agencia, en este informe, no se pronunció al respecto, parecía razonable diferenciar la

123 Agencia Española de Protección de Datos (2004). Informe 0582/2004 [en línea]. Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/transferencias_internacionales/common/pdfs/2004-0582_Subcontrataci-oo-n-de-un-encargado-del-tratamiento-en-tercer-pais-que-no-ofrece-nivel-adecuado-de-protecci-oo-n.pdf [2010, 20 de junio]

subcontratación del objeto principal del contrato de los posibles trabajos que el encargado del tratamiento pueda externalizar para el desarrollo de su actividad. Obligar a solicitar autorización del responsable del fichero para todos ellos implicaría limitar la propia libertad organizativa del encargado del tratamiento. En definitiva, podía entenderse que aquellos servicios que recibiera el encargado del tratamiento en los que se acceda a datos de carácter personal del responsable del fichero no tendrían por qué ser autorizados por éste si no se refieren al objeto del contrato entre encargado y responsable.

En este sentido, el Reglamento de desarrollo de la LOPD ha venido a desarrollar este extremo a través de su artículo 21 donde se regula la posibilidad de subcontratación de los servicios. Se establece, como regla general la imposibilidad de de subcontratar con un tercero los tratamientos encomendados, salvo que se haya autorizado esta previamente. En tal caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento, por lo que es inevitable la obligación de que dicha contratación se haya autorizado previamente.

No obstante el propio artículo regula la subcontratación de los servicios sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

- Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación. El Reglamento de desarrollo de la LOPD añade, que en los casos en los que esto sea posible, deberá también especificarse en el contrato la empresa con la que se vaya a subcontratar. En caso contrario, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
- Que el encargado del tratamiento y la empresa subcontratista formalicen a su vez un contrato. En este caso, el subcontratista será considerado a su vez encargado de tratamiento.

3.2.3 Medidas de seguridad

Es necesario determinar en el contrato cuales son las medidas concretas de seguridad que deberá implantar el encargado. Normalmente, las partes se obligarán a la puesta en marcha de las medidas recogidas por la normativa vigente, en base al nivel de seguridad que el Reglamento de desarrollo de la LOPD impone a cada fichero en función de su naturaleza.

No obstante, es posible pactar la implantación de medidas de nivel superior a lo exigido, siendo habitual en este caso la determinación de cual de las partes asumirá el coste de dichas medidas.

3.2.4 Destrucción y/o devolución

El artículo 12 de la LOPD establece que cuando se ha cumplido la prestación contractual, los datos deberán ser destruidos o devueltos al responsable del tratamiento, junto con cualquier soporte en los que consten, aunque en la práctica es posible que no se destruyan o devuelvan como mero medio de acreditación de la prestación del servicio o con vistas a posibles responsabilidades que se deriven del contrato. Por tanto, es posible que las partes modifiquen, de común acuerdo, esta obligación y así lo avala la propia Agencia Española de Protección de datos en su Informe 283/2004[124]:

«No obstante, el artículo 1.255 del Código Civil establece que "los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público."

En este sentido, será posible que el contrato pudiera estipular que el cumplimiento de la prestación pudiera entenderse condicionado a la conformidad del responsable del tratamiento con la actuación efectuada por el encargado, de modo que se indicase en el contrato que la prestación de aquél se entenderá cumplida cuando, una vez finalizada la actividad en que consistía el tratamiento encomendado al encargado del tratamiento, el responsable del tratamiento compruebe y dé su conformidad a la actuación de aquél, siempre que para el otorgamiento de dicha conformidad se establezca un plazo razonable y reducido de tiempo.

De este modo, la conservación de los datos por el encargado del tratamiento durante ese período concedido para la conformidad del responsable a su actividad podría considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, puesto que sólo tras dicha conformidad podría entenderse "cumplida la prestación" en los términos establecidos en el propio contrato».

No obstante, la entrada en vigor del Reglamento de desarrollo de la LOPD ha venido a eliminar la necesidad de incluir esta prevención, ya que en su artículo 22 dispone:

124 Agencia Española de Protección de Datos (2004). Informe 0283/2004 [en línea]. *Conservación de los datos por el encargado del tratamiento*. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2004-0283_Conservaci-oo-n-de-los-datos-por-el-encargado-del-tratamiento.pdf [2010, 20 de junio]

«Artículo 22. Conservación de los datos por el encargado del tratamiento

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

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento»

3.3 Responsabilidad

Aspecto fundamental cuya regulación suele incluirse en la redacción de los contratos que regulan la relación entre el responsable y el encargado. El artículo 12.4 LOPD regula la responsabilidad:

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

Como podemos observar, en caso de incumplimiento de las obligaciones enumeradas, se considerará que se ha producido una cesión de datos, aplicándose el artículo 11 de la LOPD.

3.4 Diferencias con el Responsable del tratamiento

La Memoria del año 2000 de la Agencia Española de Protección de Datos indica:

«Se han recibido reiteradas consultas referidas al supuesto específico en que las actividades de una determinada empresa que implican un tratamiento automatizado de datos de carácter personal (nóminas, contabilidad, etc.) son efectuadas por una Entidad asesora, sin que por la empresa se

realice un tratamiento efectivo de dichos datos. En particular, se ha planteado a quien corresponderá el cumplimiento de las obligaciones reguladas por la LOPD.

De lo establecido en la mencionada Ley debe señalarse que las obligaciones que la misma impone, en particular la de proceder a la notificación del fichero a la Agencia Española de Protección de Datos, habrán de cumplirse por parte de quien ostente la condición de responsable del fichero, definido por el artículo 3.d) de la Ley como "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento».

Pare pues claro, que es el responsable del fichero quien debe aparecer identificado en las cláusulas informativas que acompañan la recogida de datos de carácter personal así como quien debe hacer efectivos los derechos de acceso, rectificación, cancelación y oposición de los interesados. La característica que diferencia al responsable del fichero del encargado del tratamiento es la capacidad para decidir sobre la finalidad, contenido y uso del fichero. El encargado del tratamiento no es autónomo en la toma de decisiones, depende en última instancia del responsable del fichero. La Agencia Española de Protección De datos resalta esta capacidad de decisión, en uno de sus informes, como elemento diferenciador de ambas figuras en uno de sus informes, relativo a la prestación de servicios de *housing* [125]. El origen del informe es una consulta en la que se plantea si una Entidad debía implantar las medidas de seguridad de nivel medio o alto en caso de prestar un servicio de *housing* a una Entidad que trata datos de carácter personal sobre los que deben implantarse este tipo de medidas. Para responder esta cuestión, la Agencia tuvo que determinar con carácter previo si la empresa consultante tenía la condición de encargado del fichero, concluyendo:

«(…) Dado que, sin perjuicio de que en principio la consultante se limita a poner a disposición de su cliente los locales, desarrolla otras actividades, tales como, tal y como se señala en la consulta, la conectividad a Internet de los sistemas, encontrándose asimismo los datos en sus locales, debe considerarse que la Entidad consultante es encargada del tratamiento, siendo preciso dar cumplimiento al régimen establecido por el artículo 12 de la Ley Orgánica 15/1999 (…).».

125 Agencia Española de Protección de Datos (2004). Informe 0416/2004 [en línea]. *Naturaleza de encargado del tratamiento del prestador de servicios de housing.* Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2004-0416_Naturaleza-de-encargado-del-tratamiento-del-prestador-de-servicios-de-housing.pdf [2010, 20 de junio]

3.5 Diferencias con el cesionario

El artículo 11 de la LOPD establece unas excepciones al consentimiento en el caso de las cesiones o comunicaciones de datos. En este punto se hace oportuno citar la establecida en al apartado c) del artículo 11.2: «*Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo contenido, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique*».

En ese contexto, la inclusión de una excepción al consentimiento en el marco de las relaciones jurídicas entre empresas que prestan servicios a otras podría tener aplicación práctica en un campo en ocasiones coincidente con el que estamos tratando aquí. No obstante, la mayoría de los supuestos nos encontraremos ante un caso de acceso a datos por cuenta de terceros haciendo que la excepción del 11.2.c LOPD vaya siendo menos utilizada.

En este sentido Alonso afirma que:

«Por lo que respecta a la "necesariedad" de la conexión para el desarrollo, cumplimiento o control de la relación jurídica, plantea dudas interpretativas a las que ya se han aludido, y que en el fondo va a dar lugar a que este "necesariamente" sea interpretado restrictivamente por la Agencia de Protección de Datos.

Esta tendencia, que ya se detectó con la antigua LORTAD, ha dado lugar a que la mayoría de supuestos las relaciones se articulen bajo la forma de prestaciones de servicios, tratando de encontrar cobertura para excepcionar el consentimiento en el acceso a datos por cuenta de terceros que regula el artículo 12 de la LOPD.

Esta particularidad hace que en la práctica, la excepción del art. 11.2.c) haya quedado prácticamente vacía de contenido».

Por su parte Heredero Higueras o Herránz Ortiz afirman que este precepto incluye casos de consentimiento presunto o tácito, según el caso, especialmente aplicables a las relaciones bancarias.

Sin embargo este argumento doctrinal es criticado ampliamente y así Messía de la Cerda afirma que:

«Si se sostiene que este supuesto es una excepción al consentimiento, sencillamente se manifiesta que la falta del mismo no impide la validez de la cesión, de manera que se admite la posibilidad de que tal requisito no concurra en tales casos.»

3.6 Responsable del tratamiento y empleados

La Agencia Española de Protección de Datos al explicar qué debe entenderse por encargado del tratamiento, establece:

«No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero».

Lo cual parece evidente que a la vista de las diversas estipulaciones que se establecen en la normativa de protección de datos sobre el personal del responsable del fichero. En primer lugar, conforme al artículo 10 de la LOPD, el personal laboral estará sujeto al deber de secreto. Dicha obligación nace del hecho de tratar los datos de carácter personal y se mantiene aún después de haber finalizado la relación que unía al trabajador con el responsable del fichero. Por su parte, el artículo 91 del Reglamento de desarrollo de la LOPD, establece que cada trabajador estará autorizado para acceder únicamente a aquellos datos que le sean necesarios para la realización de su trabajo diario:

*«**Artículo 91. Control de acceso.***
1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder,

alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio».

Además, corresponde al responsable del fichero poner en conocimiento de aquellos usuarios que realizan tratamiento de datos los procedimientos, normas, estándares de seguridad aplicables a los mismos. Esto se traduce en la práctica en la necesidad de informar al personal de aquellas medidas establecidas en el documento de seguridad que les afecten.

V. LA TRANSFERENCIA INTERNACIONAL DE DATOS

1. Introducción

La transferencias internacionales de datos se regulan como consecuencia lógica del proceso de internacionalización económica y de la evolución tecnológica desarrollada en los últimos años. Estas posibilidades reflejadas en el crecimiento constante de las nuevas redes de comunicación constituyen un escenario en el que las transferencias internacionales de datos son cada día más frecuentes dado que existe la necesidad de comunicar datos personales a terceros estados, bien en el marco de relaciones comerciales bien como consecuencia del crecimiento de las compañías responsables de los datos que sufren procesos de internacionalización y deslocalización que implican el tratamiento de datos personales en estados diferentes a aquellos en los que fueron recabados. Evidentemente, las garantías, en materia de protección de datos de carácter personal no pueden quebrarse mediante el traslado de los tratamientos a otros estados. Por tanto, en los últimos años se ha ido desarrollando un marco normativo para las transferencias internacionales que debe ser analizado en el presente estudio.

2. Concepto

El artículo 5 del Reglamento de desarrollo de la LOPD establece que una transferencia internacional de datos es cualquier:

«Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español».

Del análisis de este precepto podemos extraer como conclusión principal que una transferencia internacional de datos puede suponer tanto un encargo del tratamiento como una cesión con la característica principal de que éstas se realizan fuera del Espacio Económico Europeo.

En este sentido, el citado precepto no aclara si la transferencias internacionales de datos pueden llevarse a cabo entre responsables de tratamiento del ámbito público o privado, por lo que se debe entender que ambos tipos de entidades pueden realizar este tipo de transferencias.

2.1 Intereses

Nos encontramos en presencia de un equilibrio delicado entre los intereses económicos, cuya defensa exige una liberalización del tráfico de todos los datos necesarios para la realización de intercambios de bienes y servicios y entre las necesidades de protección de las personas, que exigen el mantenimiento de un régimen adecuado y homogéneo de protección. En definitiva lo que se trata es de conjugar los intereses del Estado con los del comercio internacional y con los intereses de los interesados o afectados.

Por tanto, un régimen de transferencia de datos adecuado debe garantizar que el nivel de protección que ofrece el país de origen, desde el que se exportan los datos, no quede sin contenido por el traslado de estos a un país que carezca de un régimen de protección. Asimismo el sistema tampoco debe de servir como *coartada* para el establecimiento de barreras contra el comercio internacional ya que el establecimiento de controles administrativos al tráfico internacional de datos puede redundar en un entorpecimiento injustificado a la libre circulación de dicho tráfico.

2.2 Clasificación

Es posible establecer distintos criterios o clasificaciones en este ámbito. Un primera clasificación sería aquella basada en el nivel de garantía del derecho a la protección de datos de carácter personal, que el estado de destino de la transferencia ofrezca. En este punto nos encontramos transferencias realizadas a países con un nivel de protección adecuado conforme a los parámetros establecidos por nuestro ordenamiento, y las transferencias a otros países que no disponen de un adecuado nivel de protección.

No obstante la clasificación propuesta por Sancho Villa[126], basada en si la transferencia es un encargo o si, por el contrario, es una cesión es una de las más acertadas ya que a través de ella podemos distinguir las transferencias internacionales de datos en dos grandes grupos:

126 SANCHO VILLA, D. (2003). *Transferencia Internacional de Datos Personales. Agencia Española de Protección de Datos*. Madrid. Páginas 47 y siguientes.

- Aquellas que se llevan a cabo entre responsables de tratamiento y,
- Aquellas en las que interviene un encargado del tratamiento.

2.2.1 Transferencias internacionales de datos entre responsables de tratamiento

La presente modalidad corresponde con el supuesto de cesión del artículo 11 de la LOPD. Se trata de un caso que ya recogía la primera norma de la Instrucción 1/2000 de la Agencia Española de Protección de Datos[127]:

«A tal efecto, se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión de comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero».

El responsable del tratamiento, que transmite los datos, realiza una cesión o comunicación de los mismos a un tercero localizado fuera del Espacio Económico Europeo actuando dicho tercero por cuenta propia y decidiendo sobre la finalidad, uso y contenido del tratamiento, en calidad de responsable de tratamiento. Dentro de la relación jurídica entre ambas partes, estas transferencias internacionales de datos pueden realizarse:

- **A título principal.** Nos encontramos en presencia de supuestos en los que la transferencias internacionales de datos se realizan a título principal cuando la transferencia es el objeto mismo de la relación entre las partes.
- **En ejecución de un contrato en interés del afectado.** Nos encontraremos en presencia de contratos entre entidades en las que ambas actúan como responsables del tratamiento y en el que la transmisión de datos actúa como accesorio a la relación principal entre las partes.

2.2.2 Transferencia internacional de datos a un encargado de tratamiento

Las transferencias internacionales de datos se basan en el acceso a datos personales por cuenta de

127 Agencia Española de Protección de Datos (2000). «*Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos*» [en línea]. Disponible en: Http://www.csae.map.es/csi/pdf/instruccion_1_2000.pdf [2010, 23 de junio]

un tercero, en los términos del artículo 12 de la LOPD. A diferencia del supuesto anterior, esta transferencia internacional se produce cuando el responsable del tratamiento transmite los datos personales a un tercero, establecido fuera del Espacio Económico Europeo, para que realice un determinado tratamiento en su nombre y por su cuenta a cambio de una contraprestación.

3. Marco normativo

3.1 La Directiva 95/46/CE

Las transferencias internacionales de datos se encuentran reguladas en los artículos 25 y 26 de la Directiva 95/46/CE, que establecen los siguientes:

*«**Artículo 25. Principios***

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para

impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26. Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaron su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión».

3.2 LOPD

Regula las transferencias internacionales de datos en los artículos 33 y 34:

*«**Artículo 33. Norma general***

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d. Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e. Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j. Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k. Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".

3.3 Instrucción 1/2000 de la Agencia Española de Protección de Datos

Desde la entrada en vigor de la LOPD, la actuación de la Agencia Española de Protección de Datos ha generado una abundante casuística relacionada con las transferencias internacionales de datos de carácter personal. En este sentido, la Agencia Española de Protección de Datos dictó en el año 2000 la Instrucción 1/2000 con el objeto de señalar los criterios orientativos seguidos por la Agencia en relación con aquellos tratamientos que supongan una transferencia internacional de datos.
No era finalidad de esta Instrucción efectuar modificaciones o innovaciones dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, tal y como establece su Título primero: «*aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido por la Agencia para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos*». En este sentido, el Reglamento de Desarrollo de la LOPD ha incorporado gran parte del contenido de la Instrucción 1/2000.

3.4 Reglamento de Desarrollo de la LOPD

El Reglamento de desarrollo de la LOPD incorpora, a la normativa en materia de protección de datos de carácter personal, las previsiones de la Instrucción 1/2000 de la Agencia Española de Protección de Datos clarificando los criterios y procedimientos para su realización y autorización.

Además, añade algunas novedades entre las que destacan la facultad atribuida al Director de la Agencia Española de Protección de Datos para considerar que en un país existe un nivel adecuado de protección, no siendo por ello necesario solicitar la autorización de dicho órgano para que la transferencia internacional pueda tener lugar, pese a que la Comisión Europea no haya declarado que el nivel de protección resulta adecuado.

Asimismo, se permite otorgar la autorización para la transferencias internacionales de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas, también denominadas *binding corporate rules* en donde deberán constar las necesarias garantías de respeto al derecho fundamental a la protección de datos consagrado en el ordenamiento jurídico español.

4. Régimen general

Para examinar las transferencias internacionales de datos vamos a basarnos en la clasificación realizada en función del nivel de protección que los estados en los que se encuentran los destinatarios otorgan a los datos de carácter personal y que se ajusta a las previsiones del artículo 33 de la LOPD donde se recoge el régimen general establecido para las transferencias internacionales de datos.

El presente artículo establece una norma general que establece como principio general la prohibición de transmisión internacional algo que no se encuentra previsto ni en el Convenio 108 del Consejo de Europa ni en la Directiva 95/46/CE. Nos encontramos en presencia de un principio general excesivamente riguroso y que sería necesario dirigir a los términos establecidos por la Directiva 95/46/CE.

En este sentido, durante el proceso de aprobación de la Ley, se realizaron algunas enmiendas que finalmente no prosperaron, por ejemplo, la enmienda número 69 del Grupo Parlamentario Socialista que proponía como texto para el apartado 1 del artículo 33 una redacción positiva, en los siguientes términos: *«Podrá realizarse la transferencia, temporal o definitiva, de los datos de carácter personal que hayan sido recogidos para su tratamiento, con destino a cualquier país en el que exista un nivel de protección adecuado»*.

No obstante, antes de analizar las excepciones a esta norma general, es necesario analizar dos conceptos importantes en el ámbito de las transferencias internacionales.

4.1 La transferencia internacional no excluye en ningún caso la aplicación de todas las disposiciones contenidas en la LOPD

El hecho de que el destino de los datos vaya a ser su transferencia a otro estado no permite a los responsables de los ficheros afectados ignorar ninguno de los principios y garantías que establece nuestro ordenamiento. En palabras de Sancho Villa[128],

«La disposición de datos personales por parte de un responsable establecido en nuestro país, supone un tratamiento (art. 3. c LOPD) que se somete a la Ley española tal y como indica el artículo 2.1 a LOPD (a salvo de lo dispuesto en el artículo 2.1 c. Es importante subrayar que el tratamiento por el que produzca esta disposición (recogida, adquisición) deberá cumplir todas las exigencias que dispone la LOPD, con independencia de que se vaya a proceder a la transferencia internacional de los datos».

4.2 La transferencias internacionales de datos deberá notificarse en el Registro General de Protección de Datos.

Nos encontramos en presencia de una obligación que deriva de las consideraciones anteriores. El responsable del tratamiento que cree el fichero, deberá notificarlo al Registro General de Protección de Datos, tal y como se establece en el artículo 26 de la LOPD:

128 SANCHO VILLA, D. (2003). *Transferencia Internacional de Datos Personales. Agencia Española de Protección de Datos*. Madrid. Página 83.

«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».

Cuando el responsable pretenda transferir datos fuera del espacio económico europeo sin que ello conste en la declaración del fichero, deberá solicitar la modificación de la inscripción del fichero tal y como se deriva del mandato del apartado tercero del artículo 66 del Reglamento de desarrollo de la LOPD:

«En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento».

5. Nivel equiparable de protección

Al regular las transferencias internacionales de datos, el artículo 33 de la LOPD establece dos conceptos fundamentales que es preciso conocer en profundidad: nivel de protección equiparable y garantías adecuadas.

En relación a este último concepto *"garantías adecuadas"*, el antiguo Reglamento de Medidas de Seguridad (RD 1332/1994)[129] establecía en su artículo 3.1:

«El Director de la Agencia de Protección de Datos autorizará la transferencia de los mismos, siempre que el cedente de los datos acredite haber cumplido lo dispuesto en los preceptos de la referida Ley y otorgue las garantías que al efecto le sean exigidas", en especial, *"la autorización deberá ser sometida al cumplimiento de las condiciones o cargas modales que se consideren necesarias para que de la transferencia no se deriven perjuicios a los derechos de los afectados y se respeten los principios contenidos en el Título II de la Ley Orgánica 5/1992».*

129 Ministerio de Justicia. Real Decreto 994/1999 Reglamento de Medidas de Seguridad de los ficheros automatizados. Publicado en el Boletín Oficial del Estado n.º 151 de 25 de junio de 1999

Dicho establecimiento vino a ser completado por la LOPD en su artículo 33.2, donde se establecen los criterios que el Director debe tener en cuenta para decidir sobre la adecuación del nivel de protección en base a los siguientes criterios:

- Naturaleza de los datos.
- Finalidad del tratamiento.
- Duración del tratamiento.
- País de origen.
- País de destino final.
- Normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate.
- Contenido de los informes de la Comisión de la Unión Europea.
- Normas profesionales y las medidas de seguridad en vigor en dichos países.

Una vez derogado el Reglamento de Medidas de Seguridad, anteriormente citado, el Reglamento de desarrollo de la LOPD ha completado esta regulación dedicando el Capítulo II de su Título VI, a las transferencias internacionales de datos. Así, el artículo 67 del Reglamento de desarrollo de la LOPD establece:

«***Artículo 67. Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.***

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán

publicadas en el Boletín Oficial del Estado.

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos».

Como podemos observar, el Reglamento por lo tanto expresamente admite "*todas las circunstancias que puedan concurrir"*, si bien, de forma adicional, incluye una serie de criterios que podrán ser tenidos y que tienen un carácter enunciativo y no limitativo.

Por su parte, el artículo 68 del Reglamento de Desarrollo de la LOPD establece:

«***Artículo 68. Nivel adecuado de protección declarado por Decisión de la Comisión Europea.***
No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o Entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección».

En este punto, el Grupo de Trabajo del Artículo 29 (GT29), ha establecido una serie de criterios y requisitos que estima necesarios con el objeto de analizar, apreciar y determinar acerca de la existencia de un nivel de protección de datos adecuado en los estados miembros de la Unión Europea. Estos criterios se contienen en el Documento de Trabajo sobre Transferencias de datos personales a terceros países y aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado por el dicho Grupo el 24 de julio de 1998[130].

Básicamente Los objetivos de un sistema de protección de datos, y los estándares de calidad que debe ofrecer la legislación de un estado para ser considerado como adecuado, son los siguientes:

- Asegurar un nivel satisfactorio de cumplimiento de las normas.

130 Grupo de trabajo del artículo 29 (1998). Transferencias de datos personales a terceros países: Aplicación de los artículos 25 y 26 de ña Directiva sobre protección de datos de la Unión Europea.

- Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos.
- Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.
- Suspensión de la habilitación.

Por último, es necesario considerar un supuesto que ya estaba recogido en la Instrucción 1/2000 de la Agencia Española de Protección de Datos y que alude a la posibilidad de que el Director de la Agencia Española de Protección de Datos pueda, en el ejercicio de sus competencias, suspender temporalmente la habilitación para las transferencias internacionales de datos. En el caso de que se determine que el importador de datos está vulnerando las normas de protección de datos del país de destino será posible la suspensión, que se encuentra regulada en el artículo 69 del Reglamento de desarrollo de la LOPD:

*«**Artículo 69. Suspensión temporal de las transferencias.***

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea».

En relación a las transferencias internacionales de datos y, a efectos prácticos, la lista de países a los que se refiere el artículo 67.2 Reglamento de desarrollo de la LOPD, respecto a los cuales no será necesaria la autorización del Director de la Agencia Española de Protección de Datos son los siguientes:

- Estados pertenecientes al Espacio Económico Europeo[131].
- **Suiza.**
- **Argentina.**
- **Canadá.**
- **Entidades de EEUU adheridas a los principios de puerto seguro.**
- **Islas de Man.**
- **Guernsey**

6. Países que no ofrecen un nivel equiparable de protección

La regla general obliga, a aquellos responsables o encargados de tratamiento que deseen llevar a cabo una transferencia internacional de datos a un país que no garantice un nivel adecuado de protección, a solicitar una autorización al Director de la Agencia Española de Protección de Datos para llevarla a cabo. En este sentido, el criterio que seguirá el Director de la Agencia Española de Protección de Datos para la concesión de esta autorización será el de asegurarse de que la transferencia garantiza la protección de los derechos de los afectados conforme a lo establecido por el artículo 33.2 LOPD así como por lo establecido en los documentos emitidos por el Grupo del Artículo 29 (GT29).

Para la autorización de la transferencia internacional de datos, la Agencia Española de Protección de Datos solicitará:

131 Asociación creada para establecer un mercado único entre la Unión Europea y los países de la Asociación Europea de Libre Comercio -EFTA-. El número actual de socios es de veintiocho, y comprende a los países de la UE más Islandia, Liechtenstein y Noruega mientras que Suiza dispone de estatuto de observador.

- La identificación de la entidad destinataria de la transferencia.
- Las finalidades para las que se transfieren los datos.
- Las medidas de seguridad.
- La duración del tratamiento.
- El país de destino.
- Las normas sectoriales, o personales que pudieran resultar de aplicación.
- El consentimiento inequívoco del interesado para que sus datos se almacenen en un fichero ubicado fuera del Espacio Económico Europeo.
- Que la titularidad del fichero corresponda a una entidad domiciliada en territorio español.
- El compromiso de que el en tercer país no se van a utilizar los datos con fines distintos a los que motivaron su recogida.

Las transferencias internacionales de datos a **estados que no garantizan** el nivel adecuado ya fueron reguladas en la Directiva 95/46/CE en cuyo artículo 26.2 se establece que los Estados miembros podrán autorizar transferencias internacionales de datos a países que no garanticen un nivel de protección adecuado cuando el responsable del tratamiento «*ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos*».

En concreto, la Directiva dispone que dichas garantías podrán derivarse de cláusulas contractuales apropiadas. Tal y como establece la Instrucción 1/2000 existen dos tipos de contratos entre transmitente y destinatario que permitían ofrecer garantías adecuadas. Sus normas 5.ª y 6ª recogen dichas garantías que la Agencia Española de Protección de Datos, en aplicación de la LOPD ha entendido como «*adecuadas*» a los efectos de otorgar la autorización pertinente.

Si bienes cierto que mediante Sentencia de 15 de marzo de 2002 de la Sala de lo Contencioso-Administrativo de Audiencia Nacional[132], anuló los apartados 2 de la norma 3ª y 6ª de dicha Instrucción, dicha anulación se refiere únicamente en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de LOPD

La Instrucción se refiere a cualquier transferencia internacional a países no equiparables, con independencia de su finalidad así como a cualquier transferencia internacional para la finalidad de

132 Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 15 de marzo de 2002. Recurso 271/2001.

tratamiento de datos o encargo del tratamiento.

En relación al contrato descrito en la Norma 5ª, además de la necesidad de identificar a las partes y la finalidad de la transferencias internacionales de datos, la Instrucción enumera las siguientes obligaciones:

- Obligación del destinatario de tratar los datos recibidos exclusivamente para la finalidad de que se trate y conforme a Derecho español. Para ello, el contrato debe obligar al destinatario a adoptar las medidas de seguridad requeridas por la normativa de protección de datos personales vigente en España.
- Se deberá establecer la responsabilidad solidaria de ambas partes frente a los afectados, a la Agencia Española de Protección de Datos y a los órganos jurisdiccionales españoles por los posibles incumplimientos del contrato en que pudiera incurrir el destinatario
- El contrato deberá recoger la garantía de que el afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, tanto ante el transmitente como ante el destinatario.

Por otra parte, el Reglamento de Desarrollo de la LOPD y en concreto, su artículo 70, ha entrado a regular este supuesto, estableciendo las siguientes pautas:

6.1. Regla general

Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos. La autorización de la transferencia se tramitará conforme al procedimiento establecido en la Sección Primera del Capítulo V del Título IX del Reglamento de desarrollo de la LOPD. Dicho procedimiento se llevará a cabo conforme a las siguientes pautas:

- **Inicio.**

Siempre a solicitud del exportador que pretenda llevar a cabo la transferencia. La solicitud deberá

incluir:

- La identificación del fichero o ficheros a cuyos datos se refiera la transferencias internacionales de datos, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.
- La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
- La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.
- En su caso, copia del contrato entre el exportador y el importador de los datos.
- Si la autorización se pretendiera para la realización de una transferencias internacionales de datos en el seno de un grupo multinacional, deberán aportarse:
  - Las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo.
  - La documentación que acredite su carácter vinculante y su eficacia dentro del grupo.
  - La documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

- **Instrucción.**

Cuando el Director de la Agencia Española de Protección de Datos, acuerde la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el *Boletín Oficial del Estado* del anuncio previsto en dicha Ley.

Transcurrido dicho plazo, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

6.2 Contrato para la transferencias internacionales de datos

El Reglamento de desarrollo de la LOPD también reconoce la posibilidad de que la autorización sea otorgada en caso de que el responsable del fichero aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

En este sentido, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en:

- Decisión de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001.
- Decisión de la Comisión Europea 2002/16/CE, de 27 de diciembre de 2001.
- Decisión de la Comisión Europea 2004/915/CE, de 27 de diciembre de 2004.
- Cualesquiera decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

6.3 Suspensión

El Director de la Agencia Española de Protección de Datos podrá denegar o suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las siguientes circunstancias:

- Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
- Que la Entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
- Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
- Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

- Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una

situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la Sección Segunda del Capítulo V del Título IX del Reglamento de desarrollo de la LOPD conforme al siguiente procedimiento:

- **Inicio.** La suspensión será acordada por el Director de la Agencia Española de Protección de Datos para lo que dictará un acuerdo que deberá ser motivado.
- **Instrucción.** Una vez iniciado, se dará traslado del acuerdo al exportador, que en el plazo de quince días podrá realizar las alegaciones que estime convenientes.
- **Resolución.** El Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.
- **Inscripción.** La resolución del Director de la Agencia Española de Protección de Datos se trasladará al Registro General de Protección de Datos para su inscripción. Se comunicará también al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.
- **Levantamiento de la suspensión.** Se producirá tan pronto como cesen las causas que la hubieran justificado, y para ello será necesaria a su vez la resolución del Director de la Agencia Española de Protección de Datos de la que se dará traslado al exportador y al Registro General de Protección de Datos y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

6.4 Transferencias dentro de multinacionales

El Reglamento de desarrollo de la LOPD cierra la regulación de estos procedimientos haciendo referencia a la transferencia internacional de datos en el marco de grupos multinacionales. En este supuesto podrá otorgarse autorización cuando hubiesen sido adoptados por estos responsables normas o reglas internas que garanticen el respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se asegure asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la normativa en materia de protección de datos de carácter personal.

Para que proceda la autorización del Director de la Agencia Española de Protección de Datos será

preciso que las normas o reglas resulten vinculantes para las empresas del Grupo implicadas en la transferencias internacionales de datos y exigibles conforme al ordenamiento jurídico español. La autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

7. Excepciones del artículo 34 LOPD

El artículo 34 de la LOPD recoge una serie de supuestos en los que no será necesario solicitar la autorización del Director de la Agencia Española de Protección de Datos. Hablamos de supuestos en los que la importancia de los intereses en juego justifica la excepción y la autorización automática de la transferencias internacionales de datos:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

- Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un

Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".

DERECHOS ARCO

I. INTRODUCCIÓN

Los derechos de acceso, rectificación, cancelación y oposición, también conocidos como derechos ARCO o derechos de las personas o del interesado, se conforman como un conjunto de garantías que la legislación española en materia de protección de datos establece para que los titulares de los mismos puedan tener un control sobre el uso que las entidades públicas y privadas hacen de los mismos.

La gran importancia de este conjunto de derechos ha sido puesta de manifiesto por el Tribunal Constitucional español que, a través de dos sentencias (290/2000[133] y 292/2000[134]) define el derecho fundamental a la protección de los datos de carácter personal.
En este sentido es importante destacar el **fundamento jurídico séptimo** de la sentencia 290/2000 que se reproduce a continuación:

«De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos 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 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. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometido, y, por otro lado, el de oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que

133 Tribunal Constitucional, Pleno, Sentencia 290/2000 de 30 de noviembre de 2000. Recurso 201/1993
134 Tribunal Constitucional, Pleno, Sentencia 292/2000 de 30 de noviembre de 2000. Recurso 1463/2000

ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.»

Como podemos observar la exposición que el Tribunal Constitucional es totalmente coherente con los principios básicos de la protección de datos, y que ya fueron sentados con anterioridad en los primeros textos de carácter internacional en la materia, a través de los cuales se reconocía al titular de los datos personales una serie de facultades o derechos de control sobre el tratamiento de las informaciones relativas a su persona.

La Resolución (73)22 del Comité de Ministros del Consejo de Europa, sobre protección de la vida privada de las personas físicas en relación a los bancos de datos electrónicos del sector privado[135], hablaba del derecho a conocer las informaciones registradas sobre dichas personas, la finalidad para la que fueron almacenadas así como las comunicaciones que se hubieran realizado de las mismas.
En el informe explicativo de la Resolución, se establece que el derecho, de los titulares de los datos personales, a conocer las informaciones que les conciernen constituye un presupuesto necesario para la adecuada protección del derecho a la intimidad.

No obstante, es ya con las Directrices de la OCDE[136] relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales y, sobre todo, del Convenio 1085 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuando se marcan y establecen los derechos que suponen un control activo del tratamiento que realiza el responsable del fichero o tratamiento.

En este sentido, el Convenio 108 incluye una importante novedad. No se limita a reconocer al titular de los datos el acceso a los mismos sino que además, le proporciona la facultad de rectificar o cancelar aquellas informaciones que sobre su persona están siendo tratadas, con posibilidad de recurrir en caso de que su petición no sea atendida.

135 Resolución R (73) 22, de 26 de septiembre de 1973, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

136 Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad..pdf

El art. 8 del Convenio 108 denomina a estos derechos "*garantías complementarias*" a las obligaciones establecidas para el responsable del tratamiento y establece lo siguiente:

«Artículo 8. Garantías complementarias para la persona concernida
Cualquier persona deberá poder:
a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.»

En todo caso no estamos hablando de garantías de carácter absoluto ya que tal y como se establece en el siguiente artículo del Convenio 108, se permite a los Estados introducir excepciones y restricciones a las ya citadas garantías dentro de los límites establecidos por el propio Convenio:

«2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.».

Por su parte, la Unión Europea, a través de la Directiva 95/46/CE[137] sigue el camino marcado por el Convenio 108 al establecer, para el titular de los datos, unas posibilidades de control similares a las establecidas por el Convenio 108. En este punto no podemos olvidar que la Comisión Europea había emitido con anterioridad a la aprobación de la directiva distintas recomendaciones aconsejando a los Estados Miembros adherirse al Convenio 108 así como que todos los Estados Miembros disponían de legislación sobre protección de datos en el momento de la aprobación del texto comunitario, normativa que, por otro lado, se vio en la necesidad de modificar[138].

La Directiva en materia de protección de datos de carácter personal introduce además una nueva garantía: el derecho de oposición (que adquiere la cualidad de garantía), al que dedica una sección del capítulo II -condiciones generales para la licitud del tratamiento de datos personales-. En este sentido y tal y como establece la Directiva el derecho de oposición es el derecho de las personas «*a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.»*[139]

En este sentido es de destacar que los derechos de cancelación y rectificación no se catalogan como garantías independientes. Las posibilidades de rectificar, suprimir y bloquear se mencionan en el artículo dedicado al derecho de acceso, artículo 12, y casi parecen derivarse del ejercicio del propio derecho de acceso.

La rectificación, supresión y bloqueo de los datos se relacionan, de forma directa, con el principio de calidad. A diferencia de lo que ocurría en el caso del derecho de oposición, dado que cuando se rectifica, suprime o se bloquea un dato de carácter personal, resulta lícito continuar el tratamiento

137 Parlamento Europeo, Consejo. 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. Publicado en Doce N.º L 281, 23 de noviembre de 1995. Disponible en: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

138 ULL PONT, E. (2003). *Derecho Público de la Informática. Protección de Datos de Carácter Personal*. 2ª edición actualizada, UNED Ediciones. Madrid,. Página 67.

139 Artículo 15.1 de la Directiva 95/46/CE

del resto de datos personales del interesado o afectada.

Por otro lado, mientras que la oposición al tratamiento de los datos personales, afecta a todos los datos de los interesados o afectados, los supuestos tasados por el artículo 12, únicamente se refieren a datos concretos.

Tal y como establece la Directiva 95/46/CE, el derecho de oposición puede ser ejercitado frente a tratamientos concretos:

- Tratamientos destinados a la publicidad y prospección comercial.
- Tratamientos tantos públicos como privados que se realizan bajo el presupuesto de un interés legítimo (en estos casos, el interesado debe justificar su oposición).

Como podemos observar, la Directiva en materia de protección de datos de carácter personal reconoce dos derechos básicos a las personas:

- El derecho de acceso (artículo 12)
- El derecho de oposición (artículos 14 y 15)

De forma adicional, el artículo 13 de la Directiva 95/46/CE, establece excepciones y limitaciones al ejercicio de estos derechos:

«1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones Y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.»

Desde el ámbito comunitario se ha resaltado la importancia de estas garantías, hasta el punto de que han sido incluidas dentro del contenido esencial a la protección de datos. De esta forma el artículo 8 de la **Carta de los Derechos Fundamentales de la Unión Europea** (actualmente el artículo II-68 del Tratado por el que se instituye una Constitución para Europa), incorpora el derecho a la protección de datos con la siguiente redacción:

«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».

Según la profesora Guerrero Picó, en el citado artículo, a diferencia de lo que ocurre en los dedicados a otros derechos en la Carta Magna Europea «*se opta por identificar lo que podría ser una suerte de contenido esencial del mismo: el principio de licitud, el principio de finalidad, el principio del consentimiento y del fundamento legal del tratamiento, el derecho de acceso y de rectificación.*»[140].

Además Guerrero Picó añade que «*incomprensiblemente, no se citan otros principios o derechos reconocidos comúnmente como parte integrante del estándar mínimo consagrado en todos los textos jurídicos europeos. No aparece el derecho de información, el principio de calidad, el derecho de cancelación o el principio de seguridad, por mencionar algunos. Tampoco se alude al régimen especial de los datos sensibles, por lo que tal vez hubiera sido más acertado limitarse a proclamar el derecho, sin aludir a las concretas facultades que lo integran*".

140 GUERRERO PICÓ, M. (2005). *El derecho fundamental a la protección de datos de carácter personal en la Constitución Europea*. ReDCE número 4. Julio-Diciembre. Disponible en: http://www.ugr.es/~redce/REDCE4/articulos/12guerrero.htm

II. DERECHOS DE LAS PERSONAS EN LA LOPD

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, también denominada LOPD, dedica su Título III a los “derechos de las personas” (artículos. 13 a 19).

La LOPD introduce escasas novedades con respecto a su predecesora, la LORTAD. La principal novedad consiste, quizá, en la introducción del derecho de oposición que prevé la Directiva 95/46/CE, y que aunque se menciona en el Título III se define y estructura fuera del citado Título, concretamente en los artículos 6.4 y 30.4 de la LOPD.

El citado Título no solo establece los derechos de acceso, rectificación, cancelación y oposición, sino que además también asigna a las personas una serie de derechos que podemos considerar secundarios, en relación a los derechos ARCO que pueden considerarse primarios:

- Derecho de impugnación de valoraciones (artículo 13 LOPD)
- Derecho de consulta del Registro General de Protección de Datos (artículo 14 LOPD)
- Derecho a indemnización (artículo 19 LOPD)

Evidentemente estos derechos secundarios no disfrutan del mismo régimen que los derechos ARCO, ya que son éstos últimos los que conforman el núcleo del derecho fundamental a la protección de datos.

En este sentido y tal y como establece el artículo 5 de la LOPD, el Responsable del Fichero no queda obligado, a informar de la posibilidad de ejercitar los derechos secundarios, lo cual no deja de tener cierto sentido si se tiene en cuenta que sólo se ha fijado procedimiento y plazo para atender los derechos principales. Por otro lado, el Responsable del Fichero no es el encargado de facilitar el derecho de consulta al Registro, ni puede resolver, como es lógico, sobre la indemnización que en su caso corresponda al interesado.

Por último no podemos dejar de destacar que la LOPD reconoce al interesado la posibilidad de solicitar la tutela de la Agencia Española de Protección de Datos frente a los derechos de acceso, rectificación, cancelación y oposición, no de otros derechos. En este sentido la redacción del

artículo 18.2 parece lo suficientemente clara en este sentido.

«El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del Organismo competente de cada comunidad autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación».

Corresponde en este punto y antes de exponer los derecho ARCO, exponer, siquiera de forma breve en qué consistes estos derechos, de carácter secundario:

A. El derecho de **impugnación de valoraciones** se encuentra estrechamente ligado con el derecho de oposición pudiendo entenderse incluido dentro del contenido de éste. Podemos decir que esta derecho es en realidad el derecho de oposición en un supuesto concreto: cuando se han realizado valoraciones automatizadas del individuo.

El artículo 15 de la Directiva 95/46/CE, relativo a decisiones individuales automatizadas, se ubica en la sección dedicada al derecho de oposición. El texto comunitario no prohíbe de manera absoluta la toma de decisiones individuales automatizadas pero sí que incluye dos importantes excepciones que, por su parte, no se encuentran establecidas en la LOPD:

- Decisiones automatizadas que se adoptan en el marco de la celebración o ejecución de un contrato, cuando se establezcan medidas apropiadas de control por parte del interesado como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo.
- Decisiones autorizadas por una ley siempre que garantice el interés legítimo del interesado.

Es importante resaltar en este punto que el artículo 12 de la anterior ley de protección de datos, conocida como LORTAD[141], sí preveía un *"derecho a la impugnación"* cuya denominación ha pervivido en la LOPD, pero que se definía en términos muy dispares a como lo hace el artículo 15 de la Directiva, ya que decía, de forma literal:

141 Jefatura del Estado. *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*. Publicada en el Boletín Oficial del Estado n.º 262 de 31 de octubre de 1992 [en línea]. Disponible en http://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf

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

Tal y como tendremos oportunidad de ver en un capítulo posterior, el nuevo reglamento de desarrollo de la LOPD (RD 1720/2007), incluye una regulación más afín a los criterios establecidos por la Directiva y vuelve a incluirlo en el contenido del derecho de oposición.

B. El derecho de consulta[142] del Registro General de Protección de Datos permite a las personas conocer la información notificada por el responsable del fichero, relativa a sus ficheros, en el momento de inscripción de éstos, pero no así los datos concretos que están siendo tratados en los citados ficheros. Este derecho se ejercita ante la propia Agencia Española de Protección de datos o, en su caso, ante las autoridades autonómicas.

Merece la pena destacar que el artículo 13 de la LORTAD regulaba en idéntica forma que el artículo 14 de la LOPD este derecho de consulta si bien la diferencia estribaba en que el mismo figuraba recogido bajo el epígrafe de "*Derecho de información*", epígrafe poco afortunada y de fácil confusión con el principio de información, pilar básico en materia de protección de datos de carácter personal.

C. El **derecho a indemnización** aparece en aquellos casos en los que el responsable del fichero cometa un incumplimiento de las obligaciones previstas en la LOPD que ocasione daños o lesiones en bienes o derechos del interesado.

El citado derecho otorga a los interesados una acción para recurrir ante los tribunales civiles, no ante la Agencia Española de Protección de Datos. Tal y como establece Aparicio Salom, este precepto parece un mero recordatorio de que "*existe la responsabilidad patrimonial en el caso de causar perjuicios*"[143]. Hablamos en este caso de la responsabilidad contractual establecida por el artículo 1902 del Código Civil.

142 Puede ser realizado por Internet a través de la página Web de la Agencia Española de Protección de Datos: www.agpd.es

143 APARICIO SALOM, J. (2000). *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal.* Editorial Aranzadi. Elcano (Navarra). Páginas 146 y 147.

III. RASGOS COMUNES DE LOS DERECHOS ARCO

Antes de entrar en profundidad con los rasgos comunes de los derechos ARCO se hace necesario matizas que sus condiciones de ejercicio no están establecidas en la LOPD sino que nuestra norma fundamental, en materia de protección de datos de carácter personal, remite en esta materia a un desarrollo reglamentario posterior.

Durante la vigencia de la LORTAD, se aprobaron dos normas básicas en materia de ejercicio de derechos:

- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992.
- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Se hace necesario citar ambas normas ya que han continuado en vigor en todo lo que no se oponían a la actual Ley Orgánica de Protección de Datos, hasta la aprobación del nuevo reglamento.

Desde su fecha de entrada en vigor, en abril de 2008, el RD 17720/2007 (Reglamento de desarrollo de la LOPD) es la disposición de referencia en lo que se refiere al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El nuevo reglamento dedica su Título III (artículos 23 a 36) a los derechos del interesado, si bien fuera de este Título también se encuentran referencias al ejercicio de derechos, en relación a tratamiento especiales de datos:

- **Artículo 44:** Ficheros de información sobre solvencia patrimonial y crédito.
- **Artículos 50 y 51:** Tratamiento para actividades de publicidad y prospección comercial.

Las características comunes a estos derechos se regulan en el Capítulo I del Título III del Reglamento de desarrollo de la LOPD (artículos 23 a 26), que pasamos a analizar a continuación:

- Son derechos personalísimos, es decir, sólo pueden ser ejercidos por el titular del dato o por

su representante legal debidamente acreditado.

Así se establece en el artículo 23 del Reglamento de desarrollo de la LOPD. Una de las dudas que se había planteado antes de la aprobación del Reglamento de desarrollo de la LOPD era el ejercicio de derechos a través de representante. En este sentido el citado artículo establece:

«b) Cuando el afectado se encuentre en situación de incapacidad o de minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse a través de su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar 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.

Cuando el Responsable del Fichero sea un órgano de las Administraciones Públicas o de las Administraciones de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho o que deje constancia fidedigna, o mediante la declaración en comparecencia personal del interesado.»

Un supuesto interesante relacionado con el ejercicio del derecho a través de representante es el que resuelve la resolución dictada por la Agencia Española de Protección de Datos en el procedimiento de tutela TD/00619/2007[144].

En este caso, el delegado de personal de la empresa PPG IBÉRICA, S.A., ejercitó el derecho de acceso a las imágenes en que apareciese grabado cada trabajador en un periodo concreto, solicitando además información sobre el destino de las imágenes grabadas, su periodo de conservación así como el control y uso de dichas imágenes. La empresa contestó acusando recibo de la petición, a la vez que indicaba que se cumplía escrupulosamente la doctrina del Tribunal Constitucional al respecto, no haciéndose efectivo el derecho de acceso.

El delegado de personal recurrió en tutela a la Agencia indicando en sus alegaciones que tenía

144 Agencia Española de Protección de Datos (2008). Resolución de 11 de enero de 2008 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00619-2007_Resolucion-de-fecha-11-01-2008_Art-ii-culo-15-LOPD.pdf

derecho a acceder a las grabaciones realizadas de su persona y a aquellas relativas a los trabajadores a los que representaba. La Agencia desestima la petición del delegado de personal indicando:

«El resumen de las cuestiones planteadas es el siguiente:
- Los derechos de acceso, rectificación y cancelación de datos son personalísimos: no pueden ser ejercidos por el reclamante en nombre de los demás trabajadores.

- En el escrito de solicitud, el afectado debe acreditar su identidad frente al Responsable del Fichero.

- En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el Responsable del Fichero deberá solicitar la subsanación de los mismos.

- El Responsable del Fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros.

- El Responsable del Fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

En este caso, a pesar de que la solicitud no reunía los requisitos para el ejercicio del derecho de acceso y el Responsable del Fichero debería haber solicitado la subsanación de los mismos, procede desestimar la presente reclamación de Tutela de Derechos porque se solicitaba el acceso a los datos de cada trabajador, sin acreditar la condición de representante legal de esos trabajadores de acuerdo con lo establecido en el punto 1 de la Norma Primera de la Instrucción 1/1998 ya citado.»

Por lo tanto, el hecho de ejercer la presentación de los trabajadores en el contexto de la relación laboral y en determinadas circunstancias, no puede entenderse que habilita para el ejercicio en nombre de éstos de los derechos que atribuye la LOPD a los titulares de los datos.

Además, como consecuencia de este carácter personalísimo de los derechos, nos encontramos con la imposibilidad de transmitirlos a los herederos. Los derechos de acceso, rectificación, cancelación y oposición no podrán ejercerse nunca en nombre de una persona fallecida, como señalaba la

Agencia en un informe jurídico del año 2002[145]:

«En consecuencia, a la vista de lo que se ha venido exponiendo, los herederos podrán tener acceso a los datos del causante en cuanto ello suponga el ejercicio en su nombre de una acción amparada por la Ley Orgánica 1/1982 o en cuanto dicho acceso se produzca en defensa de su derecho hereditario. ***Sin embargo, tales accesos no podrán ser considerados como manifestaciones del derecho de acceso, consagrado por el artículo 15 de la LOPD.»***

El Reglamento de desarrollo de la LOPD introduce una matización en el criterio sentado por la Agencia en este informe. El artículo 2.4 del Reglamento de desarrollo de la LOPD relativo al ámbito de aplicación objetivo de la ley, establece:

«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 tratamiento 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."

Sin embargo, sorprende en este punto que la Agencia Española de Protección de Datos tutele como derecho de acceso derivado de la normativa en materia de protección de datos, la solicitud de la historia clínica de un fallecido por parte de sus familiares.

Así, en la resolución R/00260/2008, que resuelve el procedimiento de tutela TD/00775/2007, leemos[146]:

«En el presente caso, ha quedado acreditado que la reclamante ejercitó el derecho de acceso a los datos personales de su marido fallecido, Don M.M.M., mediante burofax dirigido al Hospital Universitario Río Hortega.
El ejercicio de los derechos se realiza mediante solicitud dirigida al responsable del fichero en donde consten los datos identificativos del solicitante, documento acreditativo de la identidad del interesado y la petición concreta.

145 Agencia Española de Protección de Datos (2002). Informe jurídico sobre el ejercicio del derecho de acceso por los herederos del afectado.

146 Agencia Española de Protección de Datos (2008). Resolución de 10 de marzo de 2008 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00775-2007_Resolucion-de-fecha-10-03-2008_Art-ii-culo-15-LOPD.pdf

Aunque la LOPD no obliga a que el interesado utilice cualquier medio que permita acreditar el envío y la recepción de su solicitud, es conveniente que se efectúe con estas garantías a los efectos de poder justificar el correcto ejercicio del derecho, por si posteriormente existen discrepancias con el responsable del fichero sobre la recepción de la solicitud.
Cabe señalar, que la interesada efectuó correctamente su ejercicio de acceso al historial clínico de su marido fallecido mediante burofax para acreditar la fecha de presentación y de recepción de la misma.
El afectado es el que puede optar por uno de los sistemas que señala el citado artículo 12 del Real Decreto, siempre que la configuración e implantación material del fichero lo permita.
Por todo lo expuesto, procede estimar el presente procedimiento de Tutela de Derechos.»

- Los derechos son independientes.

El artículo 24.1 del Reglamento de Desarrollo de la LOPD establece que:

«no puede entenderse que le ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro».

- El ejercicio de derechos deberá ser gratuito.

Tal y como establece el artículo 17.2 de la LOPD, «*no se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación*».

Por su parte el artículo 24.2 del Reglamento de desarrollo de la LOPD recalca el carácter gratuito de su ejercicio:

«Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.»

Continúa el tercer apartado del citado artículo prohibiendo, de forma expresa, los mecanismos de ejercicio de derechos impuestos por el Responsable del Fichero que pueden suponer un coste para el interesado. En concreto:

- El envío de cartas certificadas o semejantes[147].
- La utilización de servicios de telecomunicaciones que impliquen una tarificación adicional al afectado.

Sí se considerarán conformes a lo dispuesto por la normativa en materia de protección de datos aquellos mecanismos que permitan al interesado ejercer sus derechos a través del servicio general de atención al público o de reclamaciones mantenido por el responsable del fichero.

En estos casos, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación.

- La petición de ejercicio de derechos debe reunir ciertos requisitos formales.

Enumerados en el artículo. 25 del Reglamento de desarrollo de la LOPD, dedicado al procedimiento de ejercicio de derechos.

Como consecuencia directa del carácter personalísimo de estos derechos, el interesado deberá aportar fotocopia del Documento Nacional de Identidad o documento identificativo válido en derecho, siendo posible, la utilización de firma electrónica identificativa del afectado que eximirá de la presentación de fotocopias del Documento Nacional de Identidad o documento equivalente.

Además, la solicitud deberá contener:

- Petición en que se concreta la solicitud.
- Domicilio a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que se formula en su caso.

El nuevo reglamento suprime el requisito previsto por la Instrucción 1/1998 de de hacer llegar la petición al Responsable del Fichero por cualquier medio que permita acreditar su envío y recepción. Asimismo elimina la obligación equivalente del responsable del fichero. Sin embargo, la carga de la prueba de la adecuada contestación a la solicitud del interesado recae en el Responsable del Fichero, tal y como establece el artículo 25.5, lo cual supone una obligación implícita de establecer

147 Hasta la aprobación del Reglamento de desarrollo de la LOPD, la práctica habitual era exigir al interesado que remitiera su petición a través de correo certificado o incluso burofax, puesto de la Instrucción 1/1998 determinaba que el ejercicio del derecho debía ejercerse por cualquier medio que permitiera acreditar el envío y recepción.

mecanismos que dejen constancia de la respuesta remitida al titular de los datos.

No debemos confundir la carga de la prueba de haber contestado a una solicitud con la carga de probar que no se recibió tal solicitud. Por este motivo, hemos de tener en cuenta que, aunque el nuevo reglamento de desarrollo de la LOPD no impone al interesado la remisión de la solicitud por un medio que le permita acreditar el envío y la recepción de la solicitud, es conveniente que se realice con estas garantías.

Así lo establece la propia Agencia Española de Protección de Datos en la resolución al procedimiento de tutela TD/00736/2007:[148]

«Aunque la LOPD no obliga a que el interesado utilice cualquier medio que permita acreditar el envío y la recepción de su solicitud, es conveniente que se efectúa con estas garantías a los efectos de poder justificar el correcto ejercicio del derecho, por si posteriormente existen discrepancias con el responsable del fichero sobre la recepción de la solicitud, como en este procedimiento.

La obligación general del responsable del fichero para el ejercicio de cualquier derecho es contestar expresamente a la solicitud recibida, estimando o desestimando la petición. Esta obligación de contestación expresa procede incluso cuando no existen datos registrados relativos al solicitante, debiendo el responsable informar específicamente de la inexistencia de datos referentes al interesado en sus ficheros».

- El Responsable del Fichero, queda obligado a responder dentro de los plazos previstos en todo caso, con independencia de que se estime el derecho o se deniegue el mismo.

Asimismo deberá responder en el caso de recibir una petición de ejercicio de derechos que no cumpla los requisitos anteriores, en cuyo caso solicitará la subsanación de la solicitud.

El Reglamento de desarrollo de la LOPD regula expresamente un supuesto de cierta incidencia práctica, que no aparecía en la Instrucción 1/1998: el ejercicio de derechos ante el encargado del tratamiento.

148 Agencia Española de Protección de Datos (2008). Resolución de 28 de febrero de 2008 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00736-2007_Resolucion-de-fecha-28-02-2008_Art-ii-culo-15-LOPD.pdf

Es necesario tener en cuenta que en muchos casos el particular puede confundir a un mero prestador de servicios con la entidad responsable del fichero y que tampoco está obligado a conocer las relaciones contractuales que se han establecido entre distintas empresas o incluso entre empresas de un mismo grupo empresarial.

El artículo 26 del Reglamento de desarrollo de la LOPD dispone que en el supuesto de que los afectados ejerzan sus derechos ante el encargado del tratamiento, éste dará traslado de la petición al responsable del fichero, a menos que entre ambos exista un acuerdo que implique el ejercicio de los derechos debe realizarlo el encargado del tratamiento.

Lo que no queda suficientemente detallado en el Reglamento de desarrollo de la LOPD es si el plazo para la atención del ejercicio del derecho comenzará en el momento en que el responsable del fichero reciba efectivamente la petición o cuando la solicitud llegue al encargado del tratamiento.

- El interesado puede solicitar la Agencia Española de Protección de Datos o la autoridad autonómica que corresponda si considera que se ha vulnerado su derecho.

Esta característica común a los derechos de acceso, rectificación, cancelación y oposición no aparece recogida en el Capítulo I del Título III del Reglamento de desarrollo de la LOPD. Sin embargo, sí queda recogido en el artículo 18.2 de la LOPD. Además, el nuevo reglamento impone al responsable del fichero la obligación de informar al interesado de la posibilidad recurrir en tutela ante la Agencia Española de Protección de Datos en la misma comunicación por la que se deniega el ejercicio del derecho solicitado.

IV. EL DERECHO DE ACCESO

1 Naturaleza y contenido del derecho

Regulado en el artículo 15 de la LOPD y en los artículos 27 a 30 de su Reglamento de desarrollo, la profesora Serrano Pérez considera que el derecho de acceso tiene un carácter intermedio con respecto a los demás derechos, puesto que «*la consecuencia de acceder a los datos y tener conocimiento de su estado puede condicionar el paso siguiente*»[149].

No obstante, en la práctica, es común solicitar la cancelación de los datos o bien oponerse al tratamiento sin tener un conocimiento exacto de qué datos están siendo tratados. Además, en otras ocasiones se llega a conocer la inexactitud o incorrección de una información por medios distintos al derecho de acceso.

Si bien es cierto que es la primera garantía reconocida a las personas, el propio Reglamento de desarrollo de la LOPD señala expresamente que los derechos del interesado son independientes unos de otros.

En este sentido el artículo 27.1 del Reglamento de desarrollo define el derecho de acceso como:
«el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso se esté realizando, así como la información disponible sobre el origen de los datos y las comunicaciones realizadas o previstas de los mismos.»

Por su parte el artículo 29.3 del citado Reglamento matiza que los datos que se han de entregar serán «*todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático*».

149 SERRANO PÉREZ., M. (2005): *"El derecho fundamental a la protección de datos. Su contenido esencial"*. Los derechos fundamentales y las nuevas tecnologías. Anuario multidisciplinar para la modernización de las administraciones públicas. Nº 1, Año 2005. Dispone en http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/home.jsp

En lo relativo a qué datos puede conocer la persona que ejercita el derecho de acceso debemos remitirnos al Informe Jurídico 167/2005 sobre naturaleza y alcance el derecho de acceso[150]. En este informe se evacua a petición de una consultante que había solicitado al Servicio de Empleo el registro de aquellos usuarios que hubieran accedido a sus datos personales. El Gabinete Jurídico de la Agencia concluye que el derecho de acceso de la interesa no incluye tal información, argumentando lo siguiente:

«De este modo, el derecho concedido al interesado por la Ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de organización del Responsable del Fichero han podido tener acceso a dicha información, tal y como ha indicado ya esta Agencia Española de Protección de Datos al resolver cuestiones similares a la planteada en el presente supuesto.

A mayor abundamiento, es preciso efectuar dos consideraciones:

- En primer lugar, la legislación en materia de protección de dato únicamente exige la llevanza de un registro de accesos a los datos contenidos en un fichero en los supuestos en que, por su naturaleza, sea necesaria la implantación de las medidas de seguridad de nivel alto, establecidas en el Real Decreto 994/1999, de 11 de junio, por lo que la información solicitada por la interesada únicamente sería viable en caso de ser necesaria la implantación de dichas medidas.

- En segundo término, tal y como indica el escrito del Servicio de Empleo, la información reclamada en relación con las personas que hubieran conocido el contenido de la información de la consultante obrante en los fichero de dicho Servicio debería ser considerada como datos de carácter personal, por lo que su revelación a la interesada, persona distinta del usuario, supondría una cesión o comunicación de datos, que debería contar con el consentimiento de aquel usuario o encontrarse habilitada por la Ley, lo que no sucedería en este caso, dado el alcance que la Ley Orgánica 15/1999 otorga al derecho de acceso, al que se acaba de hacer referencia.»

150 Agencia Española de Protección de Datos (2005). Informe jurídico 0167-2005 sobre la naturaleza y alcance del derecho de acceso

Asimismo, en el procedimiento de tutela TD/00024/2007[151], la Agencia Española de Protección de Datos resuelve un supuesto similar. En este caso, un particular solicitó el acceso a los ficheros de la Agencia Estatal de la Administración Tributaria. Al ejercer el derecho, mencionaba específicamente que deseaba conocer los datos del registro de "control de accesos" relativos a aquellos usuarios del sistema de la Agencia Estatal de la Administración Tributaria que accedieron a los datos de su persona entre el 22 de mayo y 16 de octubre del año 2006. A este respecto, la Agencia establece:

«En cuanto a lo referente al acceso a la lista de control de acceso, la actuación de no otorgar tal listado en el derecho de acceso instado, es correcta por parte de la AEAT, ya que no se debe confundir el acceso a los documentos y datos que obren en el expediente administrativo, cuyo régimen se rige por la LRJPAC, con el acceso a datos personales, disponibilidad que corre por cuenta del propio interesado, entre cuya facultad no se haya el acceso a los datos de las personas que han tramitado el correspondiente expediente, al no encontrarse entre los datos que son objeto del tratamiento.»

No obstante no debemos olvidar que el derecho de acceso puede referirse a la totalidad de los ficheros tratados por el responsable o a ficheros concretos, tal y como se establece en el primer párrafo del artículo 27.2. Evidentemente, el ejercicio del derecho de acceso respecto a un fichero concreto presupone que el interesado conoce los tratamientos llevados a cabo por el responsable o al menos tiene cierta certeza de que el responsable dispone en sus ficheros de determinada información.

Con anterioridad a la aprobación del Reglamento de desarrollo de la LOPD, Pujol Montero[152], siguiendo la doctrina de Aparicio Salom, puso al descubierto los problemas que plantea el ejercicio del derecho de acceso en aquellos supuestos en los que el responsable del fichero realice tratamiento complejos, bien por la estructura propia de sus bases de datos, bien por el volumen de información que éstos contienen.

En tales casos, la Agencia venía permitiendo solicitar una aclaración del interesado «*para que señale a qué fichero se refiere su petición, no comenzando a contar el plazo del mes para la atención del derecho hasta que se haya determinado el tratamiento a que se refiere la solicitud de*

151 Agencia Española de Protección de Datos (2007). Resolución de 15 de junio de 2007 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2007/common/pdfs/TD-00024-2007_Resolucion-de-fecha-15-06-2007_Art-ii-culo-15-LOPD.pdf

152 PUJOL MONTERO, J. (2007): *"El derecho de acceso"*, Obra colectiva: «La Protección de Datos (I)». Boletín del Ilustre Colegio de Abogados de Madrid. Número 35, 3ª época, febrero de 2007. Página 104.

acceso presentada».

En este sentido el Reglamento de desarrollo de la LOPD prevé, de forma expresa, este supuesto en el segundo párrafo del artículo 27.2:

«No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.»

2 Modo en que debe hacerse efectivo

La definición del derecho que proporciona el artículo 27.1 del Reglamento de desarrollo de la LOPD supone en la práctica una guía del contenido que deberá reflejar la contestación que el responsable del fichero deberá enviar a la persona, en respuesta a su solicitud de acceso. Junto a los datos concretos objeto del tratamiento, es necesario indicar el origen de los mismos, el fin para el que se utilizan así como las cesiones realizadas o previstas.

Tal y como establece el artículo 28, el interesado, al dirigir su petición al responsable del fichero, tiene la posibilidad de elegir el método de acceso: copia remitida por correo electrónico o postal, recogida en mano, telecopia, visualización de pantalla o cualquier otro propuesto por el responsable. Cuando el responsable del fichero no facilite el ejercicio del derecho por el medio elegido por el interesado, la Agencia Española de Protección de Datos entiende que no se ha atendido correctamente el derecho de acceso.

Asimismo, el Reglamento de desarrollo de la LOPD impone al Responsable del Fichero la obligación de cumplir con las medidas de seguridad aplicables al tipo de datos objeto del derecho de acceso cuando se facilita éste al interesado. Quizá este presupuesto del Reglamento de desarrollo suponga una excesiva carga al responsable del tratamiento y, por tanto, no es descabellado que una solución legal al mismo consiste en que el propio responsable sugiera a la persona que ejercita el acceso que éste recoja los datos personalmente por razones de confidencialidad. Dado que corresponde al responsable del fichero acreditar que ha hecho efectiva la petición del interesado sea cual sea el método que éste elija para acceder a los datos, en el caso de que los datos se entreguen en mano o se facilite el acceso por visualización de pantalla, es altamente recomendable solicitar al interesado la firma de un documento que pueda utilizarse como prueba de que se ha atendido la

solicitud.

Si bien el artículo 15 de la Ley Orgánica de Protección de datos hace referencia a la gratuidad de la petición de acceso, sí es posible que el responsable del tratamiento pueda exigir el pago de aquellos gastos que resulten excesivos ya que si no es posible entender que el ejercicio del derecho de acceso supone una lesión de los intereses legítimos del responsable y que por otro lado se encuentra en consonancia con lo establecido en el artículo 12 de la Directiva 95/46/CE que estipula que el el derecho de acceso se obtiene «*libremente, sin restricciones y con una periodicidad razonable y sin retrasos* ***ni gastos excesivos***».

En este sentido, el Reglamento de desarrollo de la LOPD estipula en el último párrafo del artículo 30.3 que:

«si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.»

3 Denegación del derecho

Uno de los puntos críticos, en cuanto a estos derechos esenciales se refiere es que todas las solicitudes de ejercicio de derechos habrán de ser respondidas por el responsable del fichero, aunque adolezcan de defectos formales

Centrándonos en el derecho de acceso, conviene matizar que incluso se responderán en el supuesto de que no se esté realizando ningún tratamiento de datos relativos a la persona y sólo podrá ser negado el citado derecho en los supuestos tasados por el artículo 30 del Reglamento de desarrollo de la LOPD.

En primer lugar en un supuesto, que ya se recogía tanto en la Instrucción 1/1998[153] como en la Ley Orgánica de Protección de Datos de carácter Personal . Se podrá denegar el derecho de acceso si se ha ejercitado en los doce meses anteriores a la solicitud, salvo que el interesado acredite un interés

153 Agencia Española de Protección de Datos (1998). «*Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.*» [en línea]. Disponible en: http://noticias.juridicas.com/base_datos/Admin/i1-1998-apd.html [2011, 7 de julio]

legítimo lo cual simplemente quiere decir que el derecho de acceso sólo puede ejercerse una vez al año salvo causa justificada.

Poca fortuna tuvo aquí el legislador, dado que deja a manos de la interpretación qué debe entender se por causa justificada, ni en la Ley Orgánica ni en la Instrucción.

En este punto debemos atender a Serrano Pérez, el cual afirma que «*ante la ausencia de aclaración alguna, es de suponer que la valoración acerca de lo que constituye un interés legítimo corresponderá al responsable del fichero o del tratamiento.*[154]» A lo cual añade que cualquier petición de acceso producida antes de expirar el plazo establecido deberá entenderse legitimada si en ese plazo se ha producido algún cambio de los datos objetos de tratamiento.

Por su parte, Pujol Montero señala que «*el responsable del fichero no dispone de ninguna capacidad subjetiva para calificar el interés alegado por el interesado, solamente se limitará a verificar si la variación del dato ha de realizarse antes del plazo estipulado por la ley, plazo que constituye una interpretación algo excesiva de la Directiva que en este punto sólo habla de "periodicidad razonable", sin reducirla a ningún plazo concreto»*[155].

Para Davara Rodríguez habría resultado más adecuado no limitar de forma tan categórica este intervalo de tiempo. Para determinar qué debe entenderse por interés legítimo cita como ejemplo, el siguiente:

«un fichero de datos de un trabajador, en un órgano administrativo, que modifica los datos de acuerdo con la movilidad en el empleo y la situación personal del propio trabajador. Habría que permitir que esta persona accediese a los datos cada vez que existiese una variación de los mismos -cuestión que el interesado puede conocer en casi todas las ocasiones- como, por ejemplo, cada vez que cambie de empleo, o de situación en el mismo, o de estado e identificación domiciliaria, o de otro tipo, todo lo cual puede haber ocurrido varias veces en un año. Es posible que este caso esté recogido varias veces en el texto del artículo analizado, al decir "salvo que el afectado acredite un interés especial" e interpretamos que "un interés especial" es conocer los datos que sobre él

154 SERRANO PÉREZ, M. (2003): *El derecho fundamental a la protección de datos. Derecho español y comparado*. Thomson Civitas. Madrid. Página 353.

155 PUJOL MONTERO, J. (2007): *"El derecho de acceso"*, Obra colectiva: «La Protección de Datos (I)». Boletín del Ilustre Colegio de Abogados de Madrid. Número 35, 3ª época, febrero de 2007. Página 107.

existan en el fichero, ya que se ha producido una modificación en parte de ellos y, por tanto, puede ocurrir un error en su introducción.»[156]

El **segundo motivo** de denegación del derecho de acceso lo encontramos en el artículo 30.2 del Reglamento de desarrollo de la LOPD:

«los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al Responsable del Tratamiento revelar a los afectados el tratamiento de los datos a los que se refiere el acceso».

Por último se hace necesario destacar una novedad, introducida por el Reglamento de desarrollo de la LOPD en su artículo 30.3 que impone al responsable del fichero la obligación de informar a la persona interesada, en caso de denegación del derecho, de la posibilidad de recurrir en tutela ante la Agencia Española de Protección de Datos.

4. Plazo para atender la solicitud

Tanto el Reglamento de desarrollo de la LOPD, como la Instrucción 1/1998, establecen un doble plazo para que sean atendidas las solicitudes de acceso. Así, el artículo 29.1 del Reglamento de desarrollo de la LOPD indica que:

«el Responsable resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud».

El siguiente apartado del citado artículo continúa señalando que si la solicitud fuera estimada y la respuesta del Responsable no incluyera la información en que se concreta el derecho de acceso, éste deberá hacerse efectivo durante los **10 días** siguientes a dicha comunicación.

En este sentido se hace necesario comentar que establecer este doble plazo puede tener sentido cuando el ejercicio del derecho de acceso se haga efectivo mediante visualización en pantalla o por

156 DAVARA RODRÍGUEZ, M. (2006): *Manual de Derecho Informático*. Editorial Aranzadi. Elcano (Navarra). Página 95 y nota al pie de la página 96.

personación del interesado.

No podemos obviar que en estos casos, el Responsable del fichero se encuentra obligado a realizar una comunicación formal al interesado para informarle de que puede personarse en sus instalaciones para la entrega o visualización de sus datos. Por tanto, cuando se resuelva afirmativamente una petición de acceso, la cita para la puesta a disposición de los datos no podrá dilatarse más de diez días desde la comunicación.

Asimismo, cuando el interesado no reciba ninguna comunicación durante los 30 días siguientes a su solicitud, deberá entender desestimada su solicitud y podrá recurrir en tutela ante la Agencia Española de Protección de Datos. Se hace necesario, en este punto, profundizar en lo relativo al cómputo de los plazos aplicable a todos los derechos.

Antes de la aprobación del Reglamento de desarrollo de la LOPD, existían dudas sobre cómo había de computarse el plazo previsto para la atención del ejercicio de los derechos, puesto que en ningún punto de la normativa en la materia se determinaba si los días eran hábiles o naturales.

El Informe Jurídico 534/2003[157] de la Agencia Española de Protección de Datos, resuelve la cuestión al diferenciar entre ficheros públicos y privados para la aplicación del cómputo de plazos.

En el caso de los **ficheros privados**, era necesario recurrir a lo dispuesto en el artículo 5 del Código Civil, cuyas disposiciones se aplican como supletorias en todo lo no regulado por otras leyes. Por tanto, el cómputo de los plazos no excluirá los días inhábiles, comenzando a contarse desde el día siguiente al de la recepción de la solicitud de ejercicio de derechos.

Por el contrario, en el caso de los **ficheros públicos**, los plazos se computarán en días hábiles, puesto que en este caso resulta de aplicación la Ley 30/1992 y no así, el Código Civil.

Es cierto que los argumentos y razonamiento de la Agencia Española de Protección de Datos son realmente impecables, sin embargo, en la práctica se plantean ciertos problemas de gestión para aquellas empresas con mayor volumen de ejercicio de derechos ya que tratan una gran cantidad de datos personales. En estos casos, los Responsables del tratamiento se encontraban obligados o bien

157 Agencia Española de Protección de Datos (2003). Informe jurídico 534/2003 sobre el cómputo del plazo para la satisfacción de los derechos de rectificación y cancelación

a disponer de personal para atender los derechos en cualquier día del año, o a ver reducido considerablemente el plazo que les otorgaba la ley para responder las solicitudes.

Ante estos problemas de gestión e inaplicabilidad práctica de la normativa el nuevo Reglamento de Desarrollo de la LOPD ha variado el criterio mantenido en cuando cómputo de plazos. Así, su artículo 6 establece:

«En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando sean por meses, se computarán de fecha a fecha.»

V. EL DERECHO DE CANCELACIÓN Y RECTIFICACIÓN

1 Naturaleza y contenido de los derechos

Se encuentran regulados en el artículo 16 de la LOPD así como en los artículos 31 a 33 del Reglamento de desarrollo de la LOPD.

Ambos derechos, cancelación y rectificación tiene como rasgo común la capacidad de ser una injerencia activa en el tratamiento que realiza el Responsable del Fichero, característica que por otro lado comparten con el de oposición.

Según Serrano Pérez[158], la diferencia fundamental entre ambos es que mientras que el derecho de cancelación se ejercita cuando nos encontramos frente a un tratamiento ilegítimo de datos, el de rectificación procede cuando existe constancia de una inexactitud o carencia. Los resultados de ambos derechos también son diferentes. El primero dará lugar a la cancelación o supresión del dato. El segundo finalizará con la corrección de la información.

Parece bastante claro que el derecho de rectificación únicamente se ejercita con la pretensión de modificar datos, como indica su nombre, sin implicar la cancelación del tratamiento. Éste vendría a ser el fin del derecho de cancelación. Lo que no resulta tan evidente es que el derecho de cancelación sólo pueda ejercerse en caso de tratamiento ilegítimo de datos, como nos permite

158 SERRANO PÉREZ, M. (2003): *El derecho fundamental a la protección de datos. Derecho español y comparado*. Thomson Civitas. Madrid. Páginas 357 y 358.

comprobar una revisión de los procedimientos de tutela de este derecho resueltos por la Agencia Española de Protección de Datos.

En la práctica, el interesado suele recurrir al derecho de cancelación cuando desea que el Responsable del Fichero finalice el uso de las informaciones relativas a su persona, aunque de lo que se trate sea de revocar el consentimiento previamente otorgado o de oponerse al tratamiento de datos con fines publicitarios. Las diferencias entre derecho de cancelación, derecho de oposición y revocación del consentimiento[159] no aparecen claras en la normativa vigente, y desde luego, no resulta razonable ni posible exigir al interesado que realice un análisis jurídico de la situación antes de elegir el derecho que desea ejercer.
El derecho de rectificación se define en el artículo 31.1 del Reglamento de desarrollo de la LOPD indicando que:

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

Por su parte, el derecho de cancelación no aparece definido en este artículo, pero sí que se indica en su segundo apartado que:

«el ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento».

Como podemos observar esto supone una leve variación con lo establecido en el artículo 16 de la LOPD, donde se establece que "*la cancelación dará lugar al bloqueo de los datos*", no a la supresión de los mismos. Además el artículo 16 continúa indicando que los datos se conservarán "*únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido dicho plazo deberá procederse a la supresión*."

Esto plantea un interrogante. ¿En qué supuesto existe "deber de bloqueo" de los datos de acuerdo al nuevo reglamento? En este punto, debemos acudir a la definición de "cancelación" del artículo 5.1

159 El nuevo reglamento parece insinuar que la facultad de revocación del consentimiento previamente otorgado habrá de ejercerse a través del derecho de cancelación. Así el art. 31.2 indica en su segundo párrafo: *«En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.»*

del Reglamento de desarrollo de la LOPD:

«b) cancelación: Procedimiento en virtud del cual el Responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto pata su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la posible atención de responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidad. Transcurrido ese plazo deberá procederse a la supresión de los datos.»

El citado artículo introduce un nuevo concepto: el procedimiento por el que el Responsable cesa en el tratamiento de los datos, ya de oficio o como consecuencia del ejercicio del derecho de cancelación por el interesado. El cese en el tratamiento de los datos, implica el bloqueo de los mismos. De la definición, parece deducirse que se procederá al bloqueo de los datos cuando exista un deber de conservación de los mismos, a efectos de depurar posibles responsabilidades nacidas del tratamiento. Por tanto, el resultado al que llegamos es idéntico al establecido en el artículo 16 de la LOPD, sólo que el razonamiento resulta más complejo.

La redacción dada por el Reglamento de desarrollo de la LOPD recalca que el fin último de la cancelación es siempre el borrado de los datos. En cualquier caso, sobre todo teniendo en cuenta las dudas que había suscitado la identificación de la cancelación de datos con supresión automática de los mismos al amparo de la LORTAD y de la Instrucción 1/998.

La norma tercera de la Instrucción 1/1998, que se ha mantenido vigente hasta abril del 2008, identificaba cancelación con borrado del datos y prohibía expresamente la utilización de una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas (por ejemplo, una lista Robinson de clientes que no desean recibir publicidad). No obstante lo anterior, los dos últimos apartados de la norma tercera abrían la posibilidad a que "*en los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado*", los datos se mantengan bloqueados.

En consonancia con lo establecido en los apartados 4 y 5 de la LORTAD, la instrucción matizaba que:

«La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del

afectado o de terceros o cuando existiese una obligación de conservar los datos.»

Esta regulación resultaba, a todas luces, ambigua, puesto que no se definía qué debía entenderse por "*obligación de conservar los datos*".

Con la LOPD, el derecho de cancelación, se configura de tal manera que no da lugar al borrado o eliminación directa de los datos. En la mayor parte de los supuestos, los datos no se borrarán, sino que serán bloqueados. La identificación que hacía la Instrucción 1/1998 de cancelación y borrado de datos suscitó cierta confusión y fue objeto de análisis detallado en un informe jurídico del año 2001 sobre bloqueo de datos[160]. En dicho informe, la Agencia señalaba:

«Existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el Responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.

Por el contrario, el Responsable del Fichero estará obligado, bien por el contenido de aquélla relación jurídica, bien por lo establecido en una norma imperativa, al mantenimiento del dato, si bien sometido a determinadas condiciones que aseguren y garanticen el derecho del afectado a la protección de sus datos de carácter personal, no pudiendo disponer de tales datos en la misma medida en que podría hacerlo en caso de que no procediera (de oficio -por haber dejado de ser necesarios para el cumplimiento de la finalidad del fichero- o a solicitud del afectado) la cancelación de los mismos.»

Si bien es cierto que en el citado informe también se resaltaba que el fin último de la cancelación es la supresión de las informaciones tratadas, parece poco comprensible que el legislador vuelva en el Reglamento de desarrollo de la LOPD a la idea de que la cancelación dará lugar a que se supriman los datos, debiendo recurrirse a otro artículo, situado en un título diferente de la ley para determinar cuándo procede bloquearlos. Sin duda, y dado que se ha definido qué debe entenderse por procedimiento de cancelación, parece más adecuado hacer referencia a este procedimiento a la hora de indicar los efectos del derecho de cancelación, o simplemente mencionar que el derecho de cancelación dará lugar a que se cese en el tratamiento de los datos.

160 Agencia Española de Protección de Datos (2001). Informe jurídico 0000/2001 sobre el bloqueo de datos de carácter personal.

2 Modo en que deben hacerse efectivos

En lo relativo a las peticiones de rectificación, hemos de decir que son poco frecuentes en la práctica y no suelen resultar conflictivas para el Responsable del tratamiento. El interesado habrá de adjuntar junto a su petición la documentación que justifique el cambio solicitado. La acción del Responsable consistirá en realizar dicha corrección en los datos que trata, cuando se haya acreditado convenientemente que procede la modificación.

Sin embargo, la atención del ejercicio del derecho de cancelación presenta mayores problemas. Como hemos tenido oportunidad de ver, la cancelación no supone automáticamente el borrado de los datos. En la mayor parte de los casos, deberá procederse al bloqueo de los mismos. También se ha hecho referencia a que los supuestos en los que procede el bloqueo de los datos, se establecen en el nuevo reglamento de la LOPD, artículo 5.b), al definir qué debe entenderse por "cancelación".

En base a este artículo, el bloqueo consiste en la identificación y reserva de los datos con el fin de impedir su tratamiento, excepto su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

No obstante, el reglamento no resuelve el problema de los plazos durante los cuáles deberán mantenerse los datos bloqueados. Algo se indicaba al respecto en el citado informe sobre bloqueo de datos del año 2001:

«Debe recordarse en relación con el mantenimiento del dato bloqueado, en cuanto supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que "cumplido el citado plazo deberá procederse a la supresión"), que ha de tenerse en cuenta que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que

funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia fiscal (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En consecuencia, cabe entender que la cancelación no supone automáticamente en todo caso un borrado o supresión física de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al Responsable del Fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.»

El Reglamento de desarrollo de la LOPD tampoco aclara cómo proceder a la atención del derecho de cancelación en relación a los ficheros no automatizados. En este sentido, debemos entender válida la práctica consistente en archivar en un lugar diferenciado y con acceso restringido los documentos que se pretenden cancelar.
Es importante destacar que no basta con realizar la cancelación o modificación, sino que además resulta necesario que el Responsable del tratamiento expida una certificación dirigida al interesado en la que le comunique formalmente que se ha procedido rectificar los datos o a cancelarlos. Si no se responde de manera expresa a la petición del interesado, éste podrá entenderla desestimada y por tanto, recurrir en tutela ante la Agencia Española de Protección de Datos, tal y como establece el artículo 32.2 del Reglamento de desarrollo de la LOPD.

Tanto la rectificación como la cancelación se extienden a las comunicaciones realizadas, establecidas en el artículo 16.4 de la LOPD y en el artículo 32.2 de su Reglamento. Por tanto, el Responsable del Fichero deberá realizar las oportunas notificaciones a los cesionarios a efectos de que ellos realicen también la cancelación o rectificación. No se exige que el cesionario de los datos realice ninguna comunicación a los interesados.

3 Denegación de los derechos

Tal y como establecía la instrucción 1/1998, el derecho de cancelación podía ser denegado en tres supuestos contemplados en el apartado 5 de su norma tercera:

- En caso de que la cancelación afecte a los intereses legítimos del afectado.
- En caso de que la cancelación afecte a los intereses legítimos de terceros.
- En caso de que exista la obligación de conservar los datos.

La nueva regulación establecida en el artículo 33 del Reglamento de desarrollo de la LOPD, suprime la referencia a intereses legítimos del afectado o de terceros y establece como causas comunes para denegar los derechos de rectificación y cancelación las siguientes:

- Cuando los datos deban ser conservado durante los plazos previstos en disposiciones aplicables.
- Cuando los datos deban ser conservados en virtud de relaciones contractuales entre la persona o entidad Responsable del Tratamiento y el interesado que justificaron el tratamiento de los datos.
- Cuando así lo prevea "*una ley o norma de derecho comunitario de aplicación directa o cuando éstas impidan al Responsable de Tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso*".

En todo caso, la denegación de rectificación o cancelación de datos habrá de comunicarse formalmente al interesado.

4 Plazo para atender la solicitud

El plazo de atención para el ejercicio de los derechos de rectificación y cancelación, así como para proceder a solicitar al interesado la subsanación de la petición dirigida al Responsable del Fichero, es de 10 días hábiles a contar desde la recepción de la solicitud tal y como estblecen el artículo 16 de la LOPD y el 32.1 de su Reglamento de desarrollo.

VI. EL DERECHO DE OPOSICIÓN

1 Contenido del derecho

El derecho de oposición se transpone a la normativa española a través del artículo 14 de la Directiva

95/46/CE. Con anterioridad a esta circunstancia no aparecía regulado en la LORTAD y la Instrucción 1/1998 no se refería al derecho de oposición, por lo que ha carecido de un procedimiento específico para su ejercicio hasta la aprobación del Reglamento de desarrollo de la LOPD.

Con la entrada en vigor del nuevo reglamento, la regulación de este derecho se encuentra en los artículos 6.4 y 30.4 de la LOPD así como en los artículos 34 a 36 del Reglamento de desarrollo de la LOPD.

El artículo 34.1 del Reglamento de desarrollo de la LOPD define el derecho de oposición indicando que «*es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo*» en tres supuestos concretos:

- Cuando no sea necesario el consentimiento del interesado para proceder al tratamiento de sus datos personales
- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial
- Cuando el tratamiento tenga por finalidad adoptar una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

Este último caso, amplía las opciones de ejercicio del derecho de oposición establecidas por la LOPD, incluyendo un tercer supuesto relacionado con el derecho de impugnación de valoraciones.

Tal y como establece la LOPD, el derecho de oposición correspondía en dos circunstancias:

- En el artículo 6.4 de la LOPD, se indica que cuando no sea necesario el consentimiento del interesado para proceder al tratamiento de los datos, éste podrá oponerse al mismo amparándose en motivos legítimos y fundados de su concreta situación personal. Los casos en los que no resulta necesario el consentimiento aparecen delimitados en el apartado segundo del propio artículo 6 (por ejemplo, datos tratados como consecuencia de una relación contractual de las partes o datos que figuran en fuentes accesibles al público).
- Por otro lado, el artículo 30.4 de la LOPD dispone que cuando se traten datos con fines de publicidad y prospección comercial los interesados tienen derecho a oponerse al tratamiento previa petición y sin gastos, cancelándose los datos a su simple solicitud. La expresión, *"a su simple solicitud"*, parece insinuar que cuando la finalidad para la que se utilizan los datos

es la comercial podrá ejercerse el derecho de oposición sin alegar interés legítimo. Tal interpretación resulta, por lo demás, de sentido común ya que se consideraría abusivo exigir a una persona que no desea recibir publicidad una justificación sobre su negativa que vaya más allá del simple deseo de no ser molestado con informaciones comerciales. En idéntica sintonía, el artículo 51 del Reglamento de desarrollo de la LOPD, establece que «*los interesados tendrán derecho a oponerse previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud*.»

Por tanto parece claro que la intención del legislador es que el derecho de cancelación frente al tratamiento de los datos para fines publicitarios sea automático, es decir, no admita ninguna excepción por parte del Responsable del Fichero.

2 Modo en que deben hacerse efectivos

El nuevo reglamento parece diferenciar entre los supuestos posibles de oposición al tratamiento para determinar el modo en que corresponde hacerse efectivo el derecho.

En primer lugar, en el caso de que el interesado ejerza el derecho de oposición en relación a tratamientos que no exigían su consentimiento previo, deberá hacer constar en su solicitud los motivos en los que basa su oposición al tratamiento, tal y como establece el artículo 35.1 del Reglamento de desarrollo de la LOPD.

Por otro lado, el ejercicio del derecho de oposición en casos de tratamientos con la finalidad de publicidad y prospección comercial aparece regulado en el Título IV, relativo disposiciones especiales aplicables a determinados ficheros de titularidad privada.

Mención aparte merece el derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos, regulado en el artículo 36. Su primer apartado renombra como derecho de oposición lo que la LOPD denomina derecho de impugnación y su apartado segundo, en lugar de referirse a cuándo procede el ejercicio de oposición en estos supuestos, indica justo lo contrario, aquellos supuestos en los que el interesado podrá verse sometido a este tipo de decisiones.

En todos los supuestos, y como ocurre en los restantes derechos, el Responsable del Fichero está obligado a contestar formalmente todas las peticiones recibidas. Lo que no se establece es la obligación que sí aparecía en relación a los derechos de rectificación y cancelación de comunicar la cesación en el tratamiento a aquellos a los que se hubieran cedidos los datos del interesado.

En lo relativo a los efectos del derecho de cancelación se asemejan a los del derecho de cancelación. El artículo 35.4 establece que «*el Responsable del Fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición.*» Por tanto, es necesario entender que el Responsable del Fichero debería poner en práctica el procedimiento de cancelación para cesar en el uso de los datos de carácter personal.

3 Denegación del derecho

El nuevo reglamento no dedica un artículo específico a la denegación del derecho de oposición tal y como ocurre para el resto de derechos esenciales. Así, su artículo 35.3 simplemente dispone:

«El Responsable del Fichero o Tratamiento deberá excluir el tratamiento de los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo».

Ya se ha comentado, con anterioridad, que en el caso de oposición a tratamientos realizados con fines de publicidad y prospección comercial el derecho de oposición debería atenderse de manera automática, sin que quepa la denegación del mismo. Sin embargo, cuando los datos sean tratados sin consentimiento del interesado, se exige la acreditación de un interés legítimo para proceder a la finalización del tratamiento de los datos. Teniendo en cuenta que ni la LOPD ni su Reglamento de desarrollo de la LOPD definen qué debe entenderse por *"interés legítimo"*, debe entenderse que queda al arbitrio del Responsable del Fichero decidir sobre si las razones aportadas por el interesado son suficientes para justificar el fin del tratamiento de los datos o no lo son.

4 Plazo para atender la solicitud

El art. 35.2 del Reglamento de desarrollo de la LOPD establece un plazo de 10 días hábiles desde la solicitud para atender al ejercicio del derecho y que cambia, radicalmente, el criterio previamente

establecido por la Agencia Española de Protección de Datos en sus resoluciones de tutela.

Sólo por citar un ejemplo, encontramos estás líneas en el Plan de inspección de oficio a cadenas hoteleras[161], que indicaba:

«En este sentido, cabe reseñar que el artículo 17 de la LOPD, que remite al desarrollo reglamentario el ejercicio de los derechos, distingue entre los relacionados con los derechos de acceso y oposición y los de rectificación y cancelación como se desprende de la expresión " ..así como..." que viene a diferenciar dos bloques distintos entre unos y otros, excepto en lo que sean de aplicación las normas comunes a todos ellos. En esta línea, el plazo para atender el derecho de oposición deberá ser el de un mes, que coincide con el previsto para el derecho de acceso y se diferencia del plazo para hacer efectivo los derechos de rectificación y cancelación. Ha de señalarse que una interpretación contraria no sería conforme con la Directiva 95/46/CE, por cuanto que implicaría la inexistencia de un plazo para el ejercicio del nuevo derecho de oposición que la norma comunitaria obliga a incorporar y proteger en el derecho interno (….)».

VII. LÍMITES A LOS DERECHOS, SUPUESTOS GENERALES Y CONSECUENCIAS DERIVADAS DE LA NO ATENCIÓN

1 Limites a los derechos del interesado en los ficheros de titularidad pública

Es preciso señalar que la normativa española de protección de datos prevé un régimen especial y diferenciado para los ficheros de titularidad pública, si bien tanto el Convenio 108 como la Directiva 95/46/CE no realizan distinción alguna entre ficheros públicos y privados.

Sin embargo el legislador español ha creído conveniente establecer un régimen especial para el tratamiento de datos que se realiza por parte de las Administraciones Públicas. Como señala TRONCOSO REIGADA[162], este régimen constituye "*una adaptación de la normativa de*

161 Agencia Española de Protección de Datos (2004). *Plan de inspección de oficio a cadenas hoteleras. Conclusiones y recomendaciones* [en línea]. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/RECOMENDACIONESCADENASHOTELERASDEFINITIVAS.pdf

162 TRONCOSO REIGADA, A. (2007): *"La protección de datos personales en las administraciones públicas"*. Obra colectiva: «La Protección de Datos (I)». Boletín del Ilustre Colegio de Abogados de Madrid, número 35, 3ª

protección de datos al ámbito público y no un debilitamiento radical de los principios y de los derechos de los ciudadanos". Así, el derecho fundamental a la protección de datos tendrá contenidos distintos en el sector público y en el privado, pues en el primero ha de interpretarse sistemáticamente, en relación a otros derechos fundamentales que la Administración está obligada a garantizar a los ciudadanos.

Una de las características del régimen aplicable a los ficheros públicos se refiere a las excepciones establecidas al ejercicio de los derechos de acceso, cancelación, rectificación y oposición, recogidas en los artículos 23 y 24 de la LOPD. Por lo demás, es necesario entender que son de aplicación las reglas expuestas en los apartados anteriores.

Tal y como establece el artículos 23, existe la posibilidad de denegar a los interesados el ejercicio de los derechos de acceso, rectificación y cancelación en relación a dos grupos de ficheros públicos:

- **Ficheros de las Fuerzas y Cuerpos de la Seguridad del Estado**. Se podrán denegar los derechos de acceso, rectificación y cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de investigaciones que se estén realizando.
- **Ficheros de la Hacienda Pública**. Se podrán restringir los derechos del interesado cuando éste sea objeto de actuaciones inspectoras y cuando el ejercicio de derechos obstaculice las actuaciones administrativas necesarias para asegurar el cumplimiento de las obligaciones tributarias.

En cualquier caso, se mantiene la posibilidad de que el interesado solicite la tutela de la Agencia Española de Protección de Datos o de la Autoridad Autonómica correspondiente.

Por su parte, el artículo 24 limita la información que se facilita al interesado en el momento de la recogida de los datos. Se permite no informar al interesado de las circunstancias del tratamiento, entre ellas, la identidad del Responsable del Fichero y la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición cuando esta información impida o dificulte el cumplimiento de las actuaciones de verificación y control de las Administraciones Públicas o afecte a la Defensa Nacional.

época. Febrero. Páginas 271 a 275.

2 Supuestos Especiales de Ejercicio de Derechos

2.1 Ficheros de solvencia patrimonial y crédito

La existencia de ficheros que faciliten información sobre solvencia patrimonial y crédito está prevista en el artículo 29 de la LOPD así como en el Capítulo I del Título IV de su Reglamento de desarrollo (artículos 37 a 44). El régimen de este tipo de tratamientos (extremadamente conflictivos desde el punto de vista de la protección de datos), prevé la existencia de bases de datos comunes sobre cumplimiento de obligaciones dinerarias mantenidas por entidades independientes a aquellas con las que el titular de los datos ha contraído la deuda. En este sistema, la entidad que mantiene el fichero común es responsable de éste como conjunto y cada entidad participante lo es de los datos que aporta.

En este sentido, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al fichero común y ante las entidades acreedoras resulta habitual. Por tal motivo, el nuevo reglamento prevé expresamente un artículo dedicado a este asunto, si bien el artículo 44, a pesar de su enunciado, no regula el derecho de oposición.

En lo relativo al **derecho de acceso,** el apartado 2 del citado artículo, diferencia dos supuestos:

- Ejercicio de derechos frente al titular del fichero común. Además de todos los datos sobre el titular que figuren en el fichero común, se deberá comunicar al interesado «*las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios*».
- Ejercicio ante cualquier otra entidad participante en el sistema. Se deberán comunicar todos los datos a los que se pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda ejercer sus derechos.

En relación a los **derechos de rectificación y cancelación**, su apartado 3 establece tres supuestos:

- Titular del fichero común. Se establece, en estos supuestos, la obligación del titular del fichero común de trasladar la petición a la entidad que facilitara los datos del titular para que

ésta resuelva. En el caso de que el Responsable del Fichero común no haya recibido contestación en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

- Entidad que ha facilitado los datos al fichero común. La entidad procederá a la rectificación o cancelación de datos en sus ficheros, a notificarlo a fichero común y a dar respuesta al interesado en el plazo de 10 días desde la recepción de la petición. Pese a que el artículo 44 no indica nada al respecto, previendo sólo el caso en el que se estime el ejercicio del derecho, debe entenderse que la rectificación o cancelación de datos sólo procederá en el caso de que el interesado presente la documentación justificativa del derecho que solicita. No se tratará de una cancelación o rectificación automática a simple solicitud del titular de los datos.
- Otra entidad participante. Los participantes que no hubieran facilitados los datos al fichero común informarán de esta circunstancia al interesado y le facilitarán la identidad y dirección del titular del fichero común en el plazo de 10 días desde la recepción de la solicitud.

2.2 Ficheros de publicidad y prospección comercial

Los ficheros cuya finalidad es la publicidad y la prospección comercial se encuentran sometidos a un régimen especial previsto en el artículo 30 de la LOPD así como en el Capítulo II del Título IV del Reglamento de desarrollo de la LOPD (artículos 45 a 51). En esta regulación, ocupa un papel primordial el ejercicio de los derechos por parte de los interesados.

El nuevo reglamento dedica dos artículos específicos al ejercicio de derechos en los ficheros de publicidad y prospección comercial. En primer lugar, el artículo 50 se refiere a los derechos de acceso, rectificación y cancelación introduciéndose una novedad importante con respecto a la legislación anterior. Cuando el interesado ejerza estos derechos ante una entidad a la que se hubiese encargado la realización de una campaña publicitaria, dispondrá de un plazo de 10 días para remitir la comunicación al Responsable del Fichero, a fin de que éste responda a la solicitud del afectado igualmente en el plazo de 10 días desde que reciba la comunicación.

Por su parte, el artículo 51 está dedicado al ejercicio del derecho de oposición, si bien únicamente se limita a repetir cuestiones ya reguladas sobre gratuidad del derecho de oposición y medios que debe poner a disposición del interesado el Responsable del Fichero.
Una novedad importante es la regulación del derecho de oposición ante un tercero al que se le

hubiera encargado la realización de una campaña publicitaria, supuesto en el que se seguirán los mismos pasos que los indicados para los derechos de acceso, rectificación y cancelación.
El nuevo reglamento dedica dos artículos al ejercicio de los derechos de acceso, rectificación, cancelación y oposición en ficheros dedicados a actividades de marketing y prospección comercial.

De forma adicional, se hace necesario mencionar los artículos 48 y 49 relacionados con el ejercicio de los derechos de cancelación y oposición. En estos artículos se regula el mantenimiento y utilización de los denominados "*listados Robinson*" ya sean propios de una compañía o comunes para un sector.

El artículo 48 resuelve uno de los problemas clásicos de esta materia, en relación al mantenimiento de datos de personas que habían ejercido el derecho de cancelación. Con anterioridad a este artículo surgía la duda de si era lícito mantener un listado de estas personas, lo que suponía en la práctica continuar tratando sus datos, cuando el titular había solicitado la cancelación de los mismos (esto es, el listado Robinson interno de una empresa). En este sentido el citado artículo se pronuncia de la siguiente forma:

«los Responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad».

Por su parte, el artículo 49 regula la creación y utilización de ficheros comunes de exclusión de envío de comunicaciones comerciales. Cuando el interesado manifieste ante un concreto Responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, el Responsable deberá informar de la existencia del fichero común de exclusión, así como de la identidad y dirección del Responsable del mismo. El artículo 49 establece la obligación de quienes vayan a realizar actividades de publicidad o prospección comercial de consultar este fichero común antes de llevarlas a cabo con el objeto de excluir los datos de las personas incluidas en el fichero.

2.3 Historia clínica

Los datos relativos a la salud de las personas, incluidos en la categoría de datos especialmente protegidos por el artículo 7 de la LOPD y objeto de un régimen de protección cualificado, se

encuentran sometidos a lo dispuesto en la legislación sanitaria, que contiene disposiciones específicas sobre plazos de conservación y acceso a los datos de carácter personal.

En este sentido, lo establecido en la normativa sobre protección de datos habrá de verse completado con la Ley 41/2002[163], básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, y con las leyes autonómicas vigentes.

En lo relativo al **derecho de acceso**, se hace necesario citar el Informe 409/2004[164], sobre acceso por el titular de la patria potestad a las historias clínicas de los menores. Y es necesaria su cita puesto que la Agencia Española de Protección de Datos, matiza en este informe que el derecho de acceso a la historia clínica regulado en la Ley 41/2002:

«constituye una modalidad de ejercicio del derecho de acceso, regulado por el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, siendo, como consagra la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, parte del contenido esencial del derecho fundamental a la protección de datos y, en consecuencia, parte esencial de un derecho de la personalidad del afectado cuyos datos son contenidos, en este caso, en la historia clínica, facilitándose copia de los mismos, como en el caso planteado en la consulta, consistente en una copia del informe de la analítica efectuada».

Queda claro que no existen dos derechos entre los que el interesado pueda optar, uno reconocido por la Ley 41/2002 y otro por la LOPD, sino un único derecho que queda sometido en todo lo no regulado por la Ley 41/2002, como por ejemplo en los plazos para atenderlo, a las normas sobre protección de datos.

Por lo demás, el supuesto que da origen a la consulta es la solicitud de acceso del padre de una paciente de 17 años a su historia clínica. En su respuesta el Gabinete Jurídico de la Agencia repite el razonamiento ya expresado con anterioridad sobre ejercicio de derechos por menores e incapaces. Así, distingue entre los mayores de 14 años y los menores de ésta edad:

«Respecto de los mayores de catorce años, teniendo en cuenta lo establecido en el artículo 162.1º

163 Jefatura del Estado. *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*. Publicada en el Boletín Oficial del Estado n.º 274, de 15 de noviembre de 2002 [en línea] Disponible en: http://www.boe.es/boe/dias/2002/11/15/pdfs/A40126-40132.pdf

164 Agencia Española de Protección de Datos (2004). Informe jurídico 0409/2004 sobre acceso por el titular de la patria potestad a las historias clínicas de los menores.

del Código Civil, se plantea si ha de considerarse que el menor tiene condiciones suficientes de madurez para ejercer el derecho de acceso, debiendo, a nuestro juicio, ser afirmativa la respuesta, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 para los mayores de catorce años. (…)

De este modo, si el padre o madre de un mayor de catorce años acude a un centro sanitario solicitando un informe de analítica o cualquier dato incorporado a la historia clínica de su hijo, sin constar autorización alguna de éste, no sería aplicable lo establecido en el artículo 18.2 de la Ley 41/2002, por lo que no debería procederse a la entrega de la información en tanto no conste la autorización fehaciente del hijo. Por supuesto, salvo en los supuestos en que el hijo haya sido previamente sujeto a incapacitación.

Respecto de los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1º del Código Civil, tomando en cuanta, fundamentalmente, sus condiciones de madurez.

En consecuencia, en el supuesto expresamente planteado en la consulta, dado que la paciente, de 17 años de edad, tendría, salvo que se hubiese declarado su incapacitación, condiciones suficientes de madurez para ejercitar su derecho de acceso a la historia clínica, la entrega de datos existentes en la misma al titular de la patria potestad exigiría que previamente se hubiera conferido por la paciente la debida representación para ello, no bastando para entregar la información la mera aportación del libro de familia.»

El derecho de cancelación sobre los datos sanitarios resulta bastante habitual en la práctica y ha sido tratado en dos informes jurídicos:

- **Informe 0049/2005[165].** Derecho de cancelación sobre los datos de un paciente.

165 Agencia Española de Protección de Datos (2005). Informe jurídico 0049/2005 sobre el derecho de cancelación sobre los datos de un paciente.

- **Informe 189/2003[166].** Cancelación de datos contenidos en historias clínicas.

En ambos casos, la Agencia concluye que no es posible proceder a cancelar los datos del paciente puesto que existe un deber de conservación de los mismos de acuerdo a la normativa específica, esto es, a la Ley 41/2002. Así el artículo 17 de la citada norma dispone:
«Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.»

En este sentido el informe 189/2003 indica:

«En lo referente a la conservación de los datos y la atención de los derechos de cancelación planteados por los pacientes, en su caso, debe recordarse que el artículo 16.2 de la Ley Orgánica 15/1999 no prevé una cancelación automática de los datos por la mera solicitud del afectado en todos los supuestos (a diferencia de las previsiones contenidas en supuestos específicos, tales como el de los datos sometidos a tratamiento con fines de publicidad), sino que dispone, en su primer inciso, que "Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley".

Ello implica que en determinados supuestos, en los que la Ley legitima o incluso impone el tratamiento, no será posible acceder a la cancelación de los datos fundada en una mera solicitud del afectado. Así, por ejemplo, el interesado no podrá pretender la cancelación de los datos necesarios para el mantenimiento de una relación contractual con el Responsable del Tratamiento o de aquéllos que el Responsable está legalmente obligado a mantener.

Así sucedería en el supuesto presente, en que la Ley 41/2002 impone la obligación de conservar los datos contenidos en las historias clínicas por el plazo que resulte pertinente, nunca inferior a cinco años.

Por esta razón, la mera solicitud de cancelación de los datos no podría llevar aparejada la misma sino en los términos previstos en las normas a las que se acaba de hacer referencia».

166 Agencia Española de Protección de Datos (2003). Informe jurídico 189/2003 sobre cancelación de datos contenidos en historias clínicas.

En idéntico sentido, la Agencia de Protección de Datos de la Comunidad de Madrid[167], ha respondido a la consulta de si se deben cancelar los datos relativos a la salud contenidos en la Historia Clínica de un paciente en los siguientes términos:

«¿Cómo atender una tutela de cancelación de datos personales incluidos en la Historia Clínica de un particular?

Se ha de tener en cuenta lo previsto en el artículo 16 de la LOPD, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, 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.

Se ha de contestar en el plazo de diez días, se debe tratar de datos cuyo tratamiento no se ajuste al o dispuesto en la Ley, o sean inexactos o incompletos. De acuerdo con la Ley 41/2002, la constatación de los datos obrantes en una historia clínica queda bajo el criterio médico, y será éste el competente para considerar la trascendencia sanitaria de todos los datos, y la necesidad de que éstos queden, o no, reflejados en soporte técnico o documental, a excepción de los mínimos exigibles en la propia norma citada, en el artículo 15, que constituye el contenido mínimo de la historia clínica.

Por otro lado, los datos deben conservarse durante los plazos previstos en las disposiciones aplicables. En el caso de datos de salud, mínimo cinco años."

2.4 El derecho de cancelación de la inscripción del libro parroquial

Durante el período comprendido entre 2005 y 2009, entraron en la Agencia Española de Protección de Datos diversas solicitudes de tutela del derecho de cancelación frente a Obispados y Arzobispados españoles (Madrid, Toledo, Valencia, Sevilla, San Sebastián, Cartagena o Calahorra,

167 La Agencia de Protección de Datos de la Comunidad de Madrid, con potestad sobre ficheros públicos en la Comunidad de Madrid, dispone en su página web de una sección en la que se publica una selección de consultas respondidas. Dado que entre los ficheros incluidos dentro de su ámbito de aplicación se encuentran los ficheros de los Hospitales Públicos, se dedica especial atención a los datos especialmente protegidos. Las consultas en relación a esta categoría de datos, entre las que figuran diversas cuestiones sobre ejercicio de derechos, se encuentran en la dirección:
http://www.madrid.org/cs/Satellite?c=CM_Texto_FA&cid=1109267621323&idPage=1109266885235&language=es&pagename=APDCM%2FCM_Texto_FA%2FmuestraTextoFA_APDCM

por citar algunos ejemplos) con la intención de poner fin al tratamiento de los datos incluidos en los Registros Bautismales.

Los reclamantes, que argumentaban desear dejar constancia de su no pertenencia a la Iglesia Católica, solicitaron la cancelación de los datos relativos a su bautismo. El tratamiento de estos datos, en cualquier caso, no podría considerarse ilegítimo al realizarse al amparo de lo establecido en el Acuerdo de 3 de enero de 1979, entre el Estado Español y la Santa Sede[168] ya que reflejan un hecho histórico y consentido por los padres del interesado menor de edad.
La Agencia Española de Protección de Datos procedió a constatar que las anotaciones de los libros bautismales hacían referencia al hecho histórico del bautismo de una persona y que constituían una base de datos de carácter personal que, conforme al artículo 2.2 de la LOPD, no se encontraban excluidas del régimen de aplicación de la misma, y por tanto sujetas al principio de calidad.

Todas las resoluciones dictadas sobre este tema, hacen referencia al artículo 4.3 de la LOPD, que establece que:

«los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado».

En base a este artículo, se determinó que debía realizarse una anotación marginal en la partida de bautismo del reclamante, a fin de que se haga constar el ejercicio del derecho de cancelación.

Citaremos como ejemplo y medio de dejar constancia de todas estas resoluciones, la R/00235/2008[169] recaída en el procedimiento de tutela TD/00758/2007, abierto contra el Arzobispado de Sevilla:

«La situación se clarifica tras la Sentencia de la Audiencia Nacional de la Sala de lo Contencioso-Administrativo, de fecha 10 de octubre de 2007, según la cual "los Libros de Bautismo, por tanto, en la medida en que recogen datos de carácter personal -al menos el nombre y apellidos del bautizado y el hecho mismo de su bautismo- con arreglo a criterios preestablecidos que permitan

168 Jefatura del Estado. Instrumento de Ratificación del Acuerdo entre el Estado español y la Santa Sede sobre Asuntos Jurídicos, firmado en la Ciudad del Vaticano el 3 de enero de 1979. Publicada en el Boletín Oficial del Estado n.º 300, de 15 de diciembre de 1979 [en línea] Disponible en: http://www.boe.es/boe/dias/1979/12/15/pdfs/A28781-28782.pdf

169 Agencia Española de Protección de Datos (2008). Resolución de 5 de marzo de 2008 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00758-2007_Resolucion-de-fecha-05-03-2008_Art-ii-culo-16-LOPD.pdf

su tratamiento, tienen la consideración de fichero y están sujetos, en cuanto tales, a la legislación en materia de protección de datos."

En consecuencia con lo anterior, debe hacerse notar que el artículo 4.3 de la LOPD establece que "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado", lo que, en el caso que nos ocupa, al entenderse que los asientos registrales del Libro de Bautismo constituyen una apariencia de pertenencia a la Iglesia Católica, es legítimo que quien se sienta inquietado por el contenido de dicho asiento, quiera dejar constancia de su disconformidad a ser considerado como miembro de la misma, por lo que debe verificarse mediante anotación marginal en la partida de bautismo del reclamante, a fin de que se haga constar el ejercicio del derecho de cancelación, hecho éste que no ha sido llevado a cabo por el Arzobispado, tal y como ha quedado acreditado, por lo que procede, en consecuencia, estimar la presente reclamación de Tutela de Derechos."

Todas las resoluciones recaídas sobre este tema son cuanto menos confusas. No resulta muy lógico aplicar a un registro que contiene una anotación de valor histórico la obligación de actualización recogida en el artículo 4.3 de la LOPD, puesto que su propia naturaleza impide cualquier puesta al día de los datos (que le haría perder el carácter de histórico).

Además, impone un determinado contenido, la realización de una anotación, en un registro llevado para otras finalidades y cuya inviolabilidad está recogida por el ya citado Acuerdo de 1979. Por no hablar, además, que el artículo 4 se refiere a la obligación de cancelar o rectificar los datos de oficio, cuando el Responsable del Fichero haya tenido constancia de una inexactitud o los datos hayan cumplido con la finalidad para la que se recabaron. En este supuesto, no se produce ni una ni otra circunstancia: el interesado no alega que no recibió en su día el bautismo o ni tampoco la finalidad de la inscripción hace innecesario el dato.

2.5 Ficheros mantenidos por detectives privados

La actividad de los detectives privados suscita distintos problemas relativos al cumplimiento de la normativa de protección de datos. En el procedimiento de tutela TD/00772/2007[170] la Agencia analiza el ejercicio de derechos en relación a los ficheros mantenidos en el ejercicio de esta

170 Agencia Española de Protección de Datos (2008). Resolución de 10 de marzo de 2008 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00772-2007_Resolucion-de-fecha-10-03-2008_Art-ii-culo-15-LOPD.pdf

profesión. El interesado ejercitó el derecho de acceso a sus datos personales mantenidos en los ficheros de un Detective Privado a través de burofax.

En orden al razonamiento de la Agencia, la actividad de los detectives privados queda amparada por su normativa específica, y en concreto por la Ley 23/1992, de 30 de junio, de Seguridad Privada[171], cuyo artículo 103 establece:

«Los detectives privados están obligados a guardar riguroso secreto de las investigaciones que realicen y no podrán facilitar datos sobre estas más que a las personas que se las encomienden y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.»

En base a esto, se procedió a desestimar la petición de tutela del interesado. Es importante tener en cuenta el hecho de que se trata de un límite al derecho de acceso en un fichero de carácter privado.

2.6 Ficheros mantenidos por abogados

Analizaremos a continuación un supuesto que guarda cierta similitud con el que hemos tenido oportunidad de examinar en el apartado anterior, el ejercicio de derechos en relación a los ficheros mantenidos por abogados. Antes de profundizar, sólo realizar un apunte y que no es otro más que mencionar que la profesión de abogado se encuentra igualmente sometida al deber de secreto tal y como lo esta la de los detectives.

Como ejemplo ilustrativo se mencionará el procedimiento TD/00726/2007[172], incoado a instancia de una persona que desea conocer los datos relativos a su persona que trata un abogado. El abogado, por su parte, alega no tratar ningún dato puesto que éstos son responsabilidad de sus clientes, que son los que les facilitan la documentación necesaria para plantear la demanda.

En este caso, y de forma sorprendente, no resultó suficiente la argumentación realizada por el denunciado, que quizás habría tenido que basar su denegación al ejercicio del derecho en el deber de secreto y en el derecho de defensa que asiste a su cliente, estimando la Agencia Española de

171 Jefatura del Estado. Ley 23/1992, de 30 de julio, de Seguridad Privada. Publicada en el Boletín Oficial del Estado n.º 186, de 04 de agosto de 1992 [en línea] Disponible en: http://www.boe.es/boe/dias/1992/08/04/pdfs/A27116-27122.pdf

172 Agencia Española de Protección de Datos (2008). Resolución de 25 de febrero de 2008 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-00726-2007_Resolucion-de-fecha-25-02-2008_Art-ii-culo-15-LOPD.pdf

Protección de Dato, la petición de acceso de la parte denunciante.

Es importante en este punto recordar el Informe Jurídico de la Agencia Española de Protección de Datos sobre el tratamiento de datos por parte de abogados y procuradores del año 2000[173]. En el citado informe no se planteaba ninguna cuestión relativa al ejercicio de derechos, sino únicamente si es necesario solicitar el consentimiento del contrario para proceder al tratamiento de sus datos personales.

La Agencia señala que en este caso se produce un conflicto entre dos derechos fundamentales que es necesario ponderar:

«Para resolver esta cuestión, debe indicarse que, en primer lugar, la propia Ley Orgánica 15/1999 permite establecer los límites para la exigencia del consentimiento, dado que su artículo 6.1 exige, como regla general, el consentimiento para el tratamiento de los datos "salvo que la Ley disponga otra cosa".

A la vista de este precepto, el legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En este caso, como se dijo, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquéllos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 del Texto Constitucional.

En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de "los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener

173 Agencia Española de Protección de Datos (2000). Informe jurídico 0000/2000 sobre tratamiento por Abogados y Procuradores de los datos de las partes en un proceso.

el pleno desenvolvimiento de este derecho.

Por todo ello, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los Órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes, por lo que existirá, desde el punto de vista de la Agencia, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 de la Constitución y sus normas de desarrollo.

Dicho esto, deberá analizarse si el abogado o procurador se encuentra obligado, por imperativo del artículo 5.4 de la Ley Orgánica, a informar a los oponentes de su cliente de la existencia de un fichero o tratamiento, su responsable, su finalidad, la posibilidad que los afectados ejerciten los derechos que la Ley les atribuye y los destinatarios de los datos, dada la concurrencia entre el derecho del cliente a obtener la adecuada asistencia de letrado y, en definitiva, a ver satisfecha la tutela judicial efectiva, consagrada por el artículo 24 de la Constitución, y del oponente a la protección de sus datos de carácter personal, lo que supondrá el cumplimiento del citado deber de información.
Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) "el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".

Pues bien, aplicando la doctrina antedicha al supuesto concreto, y sin perjuicio de lo que, en su caso, manifestare en el futuro el Tribunal Constitucional, procederá ponderar en qué caso la limitación del ejercicio de uno de los derechos en conflicto puede producir una mayor merma de los derechos de la otra parte o, en su caso, las medidas que permitirán mitigar ese potencial perjuicio.

Siguiendo esta premisa, en nuestra opinión debería darse una prevalencia al derecho consagrado

por el artículo 24 de la Constitución, garantizando a su vez las medidas que evitarán un mayor perjuicio a los afectados (en este caso, los oponentes de los clientes cuyos datos son objeto de tratamiento).

Ello se funda en que la comunicación a los afectados de las informaciones de que los abogados o procuradores puedan disponer, procedentes de sus clientes, podrían perjudicar, como ya se indicó, el adecuado ejercicio por el propio interesado de las facultades vinculadas con su derecho a obtener la tutela efectiva de los Jueces y Tribunales (al quedar en conocimiento de la otra parte los datos que pudieran ser aportados a juicio en defensa de su derecho).»

Parece claro que cualquier experto en la materia podría posicionarse en idéntico razonamiento en el caso de ejercicio de derechos de acceso, rectificación, cancelación y oposición por parte de las partes de un proceso a los ficheros tratados por parte de un abogado.

2.7 El Padrón Municipal

El Padrón Municipal tiene el carácter de registro administrativo, con la consideración de fichero de titularidad pública, en el que constan los vecinos de un determinado municipio. La información contenida en el Padrón constituye prueba de residencia y de domicilio habitual. Está regulado por el Real Decreto 1690/1986, de 11 de julio, por el que se aprueba el Reglamento de Población y Demarcación de las Entidades Locales y la Ley Orgánica 14/2003, de 20 de noviembre, de reforma de la Ley Orgánica 4/2000, de 20 de noviembre[174].

Ante tal cantidad de datos personales manejados en estos ficheros es evidente que los datos contenidos en el Padrón presentan un gran interés tanto para empresas privadas y particulares como para la Administración Pública. La Agencia Española de Protección de Datos ha resuelto diversas consultas relativas al tratamiento de los mismos.

De los informes jurídicos sobre el Padrón Municipal cabe destacar el Informe 0379/2007[175], sobre

174 Ley Orgánica 14/2003, de 20 de noviembre, de Reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, modificada por la Ley Orgánica 8/2000, de 22 de diciembre; de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local; de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y de la Ley 3/1991, de 10 de enero, de Competencia Desleal.

175 Agencia Española de Protección de Datos (2007). Informe jurídico 0379/2007 sobre acceso a datos del padrón

acceso a datos del padrón por particulares, pues en el mismo se incluye un límite al derecho de acceso ejercicio por el titular de los datos.

La consulta que da lugar a este informe es la solicitud de acceso por parte de la propietaria de un inmueble a los datos contenidos en el padrón sobre anteriores propietarios del mismo. La Agencia Española de Protección de Datos considera que, de acuerdo a la normativa sobre la materia, no procede otorgar el acceso solicitado argumentando lo siguiente:

«Como regla interpretativa de lo hasta aquí enunciado, el artículo 16.3 de la propia Ley de Bases de Régimen Local redactado conforme a lo establecido en la Ley Orgánica 14/2003, de 20 de noviembre, establece que "los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia".

Fuera de estos supuestos, los datos del Padrón son confidenciales (artículo 53 del Real Decreto 1690/1986, de 11 de julio que regula el Reglamento de Población y Demarcación Territorial de las Entidades Locales) y su acceso se rige por la Ley 15/1999 y por la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La Agencia Española de Protección de Datos ha considerado que la expresión «datos del Padrón municipal» que se emplea en el artículo 16.3 de la LBRL se refiere únicamente a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio. Por ello, cualquier comunicación o cesión de los datos del Padrón deberá fundarse en la necesidad por la Administración cesionaria, en el ejercicio de sus competencias, de conocer el dato del domicilio de la persona afectada, dado que del artículo 4.2 de la Ley se deriva la imposibilidad del tratamiento de los datos para fines diferentes de los que motivaron su recogida, salvo que así lo consienta el afectado o la Ley lo prescriba.

---

por particulares.

Al propio tiempo, de lo dispuesto en el citado artículo 16 de la Ley reguladora de las Bases del Régimen Local se desprende que los datos del Padrón Municipal únicamente podrán ser comunicados, con la extensión y para las finalidades que se han venido indicando, a las Administraciones Públicas, sin que dicha norma habilite a su transmisión a personas o entidades privadas, como la que se indica en la consulta.»

2.8 Buscadores de Internet

Sobre este punto es importante comentar dos resoluciones de tutela de derechos, una de la Agencia Española de Protección de Datos y otra de la Agencia de Protección de Datos de la Comunidad de Madrid que se pronuncian sobre la posibilidad de los particulares de solicitar la exclusión de datos relativos a su persona de las listas de resultados de los buscadores de Internet.

En el procedimiento de tutela Procedimiento Nº: TD/00463/2007[176], una persona ejerce el derecho de oposición frente a Google Spain, S.L. fundándolo en el interés legítimo de que no apareciera su nombre ligado a *"un hecho de notorio rechazo social"*: una resolución sancionadora de un ayuntamiento por infracción de una ordenanza ciudadana. Esta resolución aparecía publicada en el Boletín oficial de la Provincia correspondiente, que había sido puesto on-line por la Diputación.

El denunciante consideraba que al tener estos datos la condición de fuentes accesibles al público, la publicación por parte de Google debería cesar desde el momento en el que ejerciera su derecho de oposición. Por su parte, el buscador indicó que "*la solución dependía del bloqueo de la página de donde salen los resultados, por el titular de la Web referenciada (es decir, por la Diputación Provincial en cuestión)*".

La resolución, que estima el derecho de oposición ejercicio (recurrida por Google), comienza señalando que Google entra dentro de la definición de prestador de servicios de la Sociedad de la Información y por tanto le es de aplicación lo dispuesto en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)[177].

176 Agencia Española de Protección de Datos (2007). Resolución de 20 de noviembre de 2007 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2007/common/pdfs/TD-00463-2007_Resolucion-de-fecha-20-11-2007_Art-ii-culo-17-LOPD_Recurrida.pdf

177 Jefatura del Estado. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Publicada en el Boletín Oficial del Estado n.º 166, de 12 de julio de 2002 [en línea] Disponible en:

A continuación, la Agencia señala que el artículo 8 de la LSSI determina que en caso de que un concreto servicio de la sociedad de la información atente o pueda atentar contra el respeto a la dignidad de la persona, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran.

Teniendo en cuenta que el supuesto planteado puede afectar a la dignidad de la persona, la Agencia considera que es competente para decidir en este caso al incluir el derecho a la protección de datos matices más amplios que la intimidad personal que se relacionan con la dignidad de la persona. A este efecto, cita la Sentencia del Tribunal Constitucional STC 292/2000[178] cuando indica refiriéndose al derecho fundamental a la protección de datos que:

« (…) *por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de Oct., FJ 4) como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona»*.

En este sentido nos interesa resaltar el planteamiento que realiza en el fundamento de derecho décimo de la resolución:

«Es necesario insistir en los efectos divulgativos multiplicadores que se producen a través de Internet y, en mayor medida de los buscadores y su repercusión en la protección de datos de las personas, especialmente sin trascendencia pública como el caso que nos ocupa, según se ha resuelto recientemente en la TD/266/2007: "Por todo ello, cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación

http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

178 Tribunal Constitucional, Pleno, Sentencia 292/2000 de 30 de noviembre de 2000. Recurso 1463/2000

universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal". Por ello debe estimarse la procedencia de evitar -mediante la estimación de la oposición al tratamiento de los datos en el caso que así lo solicite el afectado, como en el presente-, que el tratamiento por parte de un buscador tenga efectos no deseados con carácter permanente en contra de la voluntad del afectado.»

La Agencia de Protección de Datos de la Comunidad de Madrid resolvió un supuesto similar referido al derecho de cancelación[179]. En este caso, la denunciante solicita la tutela del derecho de cancelación ejercido frente a la Dirección General de Servicios Sociales de la Consejería de Familia y Asuntos Sociales, indicando que aparecían incluidos en los resultados de distintos buscadores el Boletín Oficial de la Comunidad de Madrid en el que se publicó su nombre, DNI y dirección, así como una reseña alusiva a la prestación de renta mínima de inserción social.

La Agencia de Protección de Datos de la Comunidad de Madrid considera que la cesión de datos por parte de la Dirección General de Servicios Sociales al Boletín Oficial y su publicación en el mismo sin consentimiento de la interesada resulta conforme a la legislación vigente. Sin embargo, esto no implica que deba denegarse el ejercicio del derecho de cancelación al titular de los datos. Así, determina:

«Sin embargo, el hecho de que se pueda obviar el consentimiento para el tratamiento de los datos de la reclamante, no implica necesariamente que el derecho de cancelación del titular de los datos no pueda ser ejercitado en estos casos, respecto de la publicación de los mismos en una fuente de

179 Agencia de Protección de Datos de la Comunidad de Madrid: «Los datos publicados en Diario Oficial, a través de formato electrónico, podrán cancelarse cuando haya desaparecido la causa que motivó su publicación» [en línea]. Disponible en: http://www.madrid.org/cs/Satellite?c=CM_Texto_FA&cid=1142414842815&idPage=1109179336864&language=es&pagename=APDCM%2FCM_Texto_FA%2FmuestraTextoFA_APDCM

acceso público. Y se especifica que el derecho de cancelación a que nos referimos, lo es sólo respecto de los datos publicados en el Boletín Oficial de la Comunidad de Madrid, y no respecto de los incluidos en el procedimiento administrativo que da lugar a la publicación, ya que debemos distinguir entre el tratamiento de los datos de la Sra. XXX en el marco del procedimiento administrativo, necesario para el desarrollo de las funciones propias de la Administración, del hecho de la publicación de los mismos en un Boletín Oficial, aunque este último tratamiento sea resultado de la consecución de una finalidad propia del procedimiento administrativo, cual es la de notificar a la interesada uno de los actos acaecidos en el mismo.

Pues bien, respecto a la posibilidad de admitir el derecho de cancelación de los datos de la Sra. XXX publicados en el Boletín Oficial de la Comunidad de Madrid, debemos tener en cuenta dos aspectos diferentes:

Uno.- El motivo de la publicación, es decir, la necesidad de notificar un acto en el curso de un procedimiento administrativo. En este caso, la finalización del propio procedimiento administrativo, mediante una resolución firme, conllevaría la desaparición del motivo que provocó la publicación. Con lo cual, finalizado el procedimiento, desaparece la necesidad de dar publicidad al acto que requirió la publicación para dar continuidad al propio proceso administrativo.

Dos.- El Boletín Oficial de la Comunidad de Madrid es una publicación diaria, que se efectúa tanto en formato papel, como en formato electrónico. Las dificultades de cancelación de los datos en el caso de la publicación en papel son evidentes, máxime cuando estamos ante un hecho consumado, el Boletín de 00/00/2004, y los ejemplares de los Boletines Oficiales en los que figuran los datos de la reclamante forman parte ya de las hemerotecas. Sin embargo la publicación en formato electrónico no pierde actualidad, y la posibilidad de visualizar los contenidos de Boletines Oficiales de años atrás, a través de Internet, es algo habitual y que da actualidad y permanencia a datos que ya no son actuales, y que no debieran tener permanencia, como es el hecho de una notificación de un procedimiento administrativo finalizado.

Conjugando ambos aspectos, se debe concluir que sería conforme a derecho la admisión del derecho de cancelación de la reclamante respecto de sus datos de Nombre, apellidos, DNI y domicilio, publicados en formato electrónico en el Boletín Oficial de la Comunidad de Madrid de 00/00/2004, referidos a la notificación de 00/00/0000 de la Consejería de Familia y Asuntos Sociales, siempre y cuando en el procedimiento que motivó la notificación del acto administrativo

haya finalizado con resolución firme.»

2.9 Videovigilancia

La Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[180], dedica su artículo 5 al ejercicio de derechos:

«1. Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al Responsable del Tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

2. El Responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

3. El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.»

Como podemos observar, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición sobre imágenes grabadas por cámaras de seguridad suscita innumerables dudas en su aplicación práctica. Un informe del Gabinete Jurídico de la Agencia Española de Protección de Datos, se refiere de forma expresa al ejercicio de derechos en este contexto[181].

Dicho informe presenta un análisis detallado del ejercicio de los cuatro derechos en los ficheros generados por videocámaras de seguridad:

180 Agencia Española de Protección de Datos (1998). «Instrucción 1/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios» [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/A.14-cp--Instrucci-oo-n-1-1996-.pdf [2011, 16 de julio]

181 Agencia Española de Protección de Datos (2007). Informe jurídico 0252/2007 sobre cuestiones de videovigilancia y ejercicio de derechos.

- En relación al derecho de **acceso**, el informe recuerda lo establecido por el artículo 5 de la instrucción 1/2006, para resaltar la necesidad de conciliar la atención al ejercicio del derecho de acceso de un interesado con el derecho de otras personas que aparezcan en las grabaciones a que sus imágenes no sean comunicadas a terceros. Este es el motivo por el que se permite hacer efectivo el derecho de acceso mediante certificación en la que consten los datos que son objeto de tratamiento.
- En relación a la **cancelación**, el informe señala, de acuerdo al artículo 16.2 de la Ley, que «*para que se proceda a la cancelación de las imágenes, el afectado debería de acreditar que sus datos resultan inexactos o incompletos, cuestiones que resultan difíciles de acreditar en las imágenes. No obstante, si un particular solicita la cancelación de sus imágenes, el Responsable del Fichero debería de cancelar las imágenes en el plazo de 10 días desde que se produce la solicitud. Sin embargo, sí las grabaciones son canceladas cada 24 horas, implicaría que los datos de carácter personal del solicitante han resultado ya cancelados, y el responsable del fichero deberá de informar al afectado que sus datos ya han sido cancelados.* »

  En el caso de que se haya producido una incidencia de seguridad, los datos podrán conservarse bloqueados.
- En lo relativo al derecho de **oposición**, el informe únicamente indica que es necesario que se alegue un motivo fundado y legítimo, relativo a la situación personal de cada afectado, «*para poder valorar si procede o no, por tanto al desconocer los supuestos en los que se plantea la oposición, no podemos otorgar una solución concreta*».
- Sobre el derecho de **rectificación**, se indica que no procederá atender el ejercicio del mismo al tratarse de imágenes los datos que se pretenden erróneos (“*nuestra imagen es la que es*”). Esto no implica que el Responsable del Fichero no deba atender la solicitud del afectado y fuera del plazo de cinco días que establece el apartado segundo de la Norma tercera de la mencionada Instrucción que señala «*Los derechos de rectificación y cancelación se harán efectivos por el Responsable del Fichero dentro de los cinco días siguientes a la recepción de la solicitud*».

3 Consecuencias Derivadas de la no Atención al Ejercicio de los Derechos

La importancia de los derechos de acceso, rectificación, cancelación y oposición queda reflejada en nuestro ordenamiento a través de una regulación excesivamente garantista para el afectado. En primer lugar, como hemos visto, se habilita un procedimiento para su tutela, diferente al procedimiento sancionador por incumplimientos de la normativa. Los interesados a los que se les niegue su derecho, se les facilite parcialmente o de manera deficiente pueden acudir a la Autoridad de Protección de Datos y obtener una resolución en la que se obligue al Responsable del Fichero a hacer efectivo el derecho.

Además, la LOPD establece como Infracción grave (artículo 44.3 e) de la LOPD), el impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición y que puede llegar a ser sancionada con una multa de 40.001 a 300.000 euros, con la nueva redacción articulada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible[182].

182 Jefatura del Estado. Ley 2/2011, de 4 de marzo, de Economía Sostenible. . Publicada en el Boletín Oficial del Estado n.º 55, de 5 de marzo de 2011 [en línea] Disponible en: http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf

SEGURIDAD

El principio de seguridad de los datos se estructura el artículo 9 de la LOPD e impone al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

El presente principio se configura como uno de los pilares del derecho fundamental a la protección de datos de carácter personal y por tanto, conviene profundizar en su estudio. Por tanto, el presente capítulo se centrará en el análisis y estudio de la regulación relativa al principio de seguridad, tanto desde el ámbito europeo, como desde el punto de vista de la normativa nacional.

Tal y como postula el Profesor Santamaría Ramos[183]:

«En la actualidad y, después de que la LOPD conviviese más de ocho años con el Reglamento de Medidas de Seguridad de la anterior Ley en materia de protección de datos de carácter personal conocida como LORTAD, nos encontramos con el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de carácter personal que, establece de forma rigurosa las medidas de seguridad, tanto técnicas como organizativas que son necesarias adoptar en función de la naturaleza de los datos objeto de tratamiento».

I. PRINCIPIO DE SEGURIDAD. ANTECEDENTES HISTÓRICOS

1. El principio de seguridad en la LORTAD

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, también conocida como LORTAD, fue el primer texto legal en nuestro país que reconoció el principio de seguridad. Su artículo 9, disponía:

*«**Artículo 9. Seguridad de los datos.***

1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración,

[183] SANTAMARÍA RAMOS, F.J. (2011). *El encargado independiente. Figura clave para un nuevo derecho de protección de datos.* Madrid: Wolters Kluwer España.

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.

2. No se registrarán datos de carácter personal en ficheros automatizados 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 automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley».

El presente artículo se encuentra totalmente inspirado en los textos internacionales de la materia que nos ocupa y sobre los cuales nos centraremos en los próximos epígrafes.

1.1. Consejo de Europa

Los primeros textos europeos dedicados a la protección de los datos de carácter personal fueron aprobados por el Consejo de Europa a principios de los años 70:

Tanto la Resolución R (73) 22[184] como la Resolución R (73) 23[185] incluían una mención específica a la necesidad de adoptar *"medidas técnicas y organizativas"* de seguridad para prevenir abusos en el tratamiento de los datos de carácter personal. En concreto, la R (73) 22 señala como principio número 8 que los bancos electrónicos de datos deben estar equipados con sistemas de seguridad que denieguen el acceso a personas no autorizadas:

«Precautions should be taken against any abuse or misuse of information.
Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.»

184 Relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

185 Sobre medidas de armonización en el ámbito de la informática jurídica en los Estados miembros del Consejo de Europa

1.2. El Convenio 108

El Convenio 108 constituye el antecedente más inmediato de la LORTAD. En este sentido Del Peso[186] afirma:

«El Convenio 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal establece una serie de principios básicos para la protección de los datos de carácter personal.

La Ley Orgánica de Regulación del Tratamiento Automatizado de los datos de carácter personal, de forma coherente con la incorporación del citado Convenio a nuestro ordenamiento interno, al ser ratificado el 27 de enero de 1984, recoge estos principios en los que, según se dice en la Exposición de Motivos de la Ley, ha cristalizado la opinio iuris, generada a los largo de dos décadas, y define derechos y garantías encaminados a asegurar la observancia de tales principios generada».

El artículo 7 del Convenio 108, del Consejo de Europa dispone la necesidad de establecer medidas que garanticen la seguridad de los datos:

«Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos».

Parece patente, por tanto, que la preocupación por la seguridad de los datos ya se encontraba presente en las primeras regulaciones europeas en materia de protección de datos de carácter personal si bien, el principio de seguridad aún no es más que un mero proyectos sin relevancia significativa.

1.3. Directrices de la OCDE

Otro antecedente del principio de seguridad puede encontrarse en las Directrices de la OCDE emitidas en 1980. El 23 de septiembre del citado año, la OCDE adoptó sus *Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales*, donde se señala:

186 DEL PESO NAVARRO, E. y RAMOS GONZÁLEZ, M.A. (1998): *LORTAD, Análisis de la Ley*. Ediciones Díaz de Santos. Madrid. Página 94.

«***Principio de salvaguardas de seguridad***

Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados»

1.4 Las Directrices de la ONU

Las Directrices dictadas por la ONU en el año 1990, para la regulación de los archivos de datos personales informatizados también inciden en este aspecto. En el artículo 7 de las citadas Directrices[187], podemos encontrar una referencia al principio de seguridad:

«***7. Principio de seguridad***

Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.»

No obstante la presente formulación no quedo exenta de problemas ya que su puesta en práctica no era ni mucho menos fácil y, por lo tanto, se hizo necesario regular los detalles de las medidas de seguridad que los responsables de los ficheros deberían implantar.

Todos y cada uno de los textos que acabamos de repasar marcaban pautas generales de actuación. Por tanto, tenían un marcado carácter genérico que obligaba a los Estados a legislar. En el caso de España, la LORTAD no se pronunció de forma expresa y dejó el presente tema a un posterior desarrollo reglamentario.

En este sentido la Memoria de 1994 de la Agencia Española de Protección de Datos[188] trata, de forma amplia, el principio de seguridad de los datos personales, justamente por esta falta de concreción Reglamentaria que no se corrigió hasta el año 1999, y que en aquella época necesitaba ya de un guía y un marco de actuación en materia de seguridad de los sistemas de tratamiento automatizado de datos de carácter personal.

187 Asamblea General de las Naciones Unidas (1990). Resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

188 Agencia Española de Protección de Datos. Memoria del año 1994, [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2002/common/pdfs/MemoriaApd1994.pdf

En la citada Memoria, se confirma la relación existente entre los textos internacionales y el artículo 9 de la LORTAD:

«Un punto de partida natural en este proceso de interpretar el alcance de las previsiones contenidas en la Ley en materia de seguridad de datos personales es poner en relación los objetivos de seguridad enunciados por el artículo 9.1 con los generalmente aceptados por la doctrina académica y práctica profesional en el ámbito de la seguridad de sistemas de información. En este sentido, puede establecerse un paralelismo muy estrecho entre unos y otros.

Así, el citado precepto establece como objetivos de seguridad evitar la alteración, pérdida, tratamiento o acceso no autorizado.

Es fácil establecer una correspondencia directa con los tres objetivos clásicos de la seguridad de los sistemas de información: integridad, disponibilidad y confidencialidad.

En efecto, tomando como referencia las definiciones aportadas por el documento Líneas Directrices de la OCDE para la Seguridad de los Sistemas de Información (Recomendación del Consejo de la OCDE, de 26 de noviembre de 1992), se entiende por integridad de los datos o informaciones el hecho de ser exactos y completos, y la preservación de este carácter; por disponibilidad, el hecho de ser accesibles y utilizables en el tiempo deseado y del modo requerido; y por confidencialidad, el estar únicamente al alcance del conocimiento de las personas o entidades autorizadas, en los momentos autorizados y de una manera autorizada. Y, de acuerdo con las citadas Directrices, la seguridad de los sistemas de información tiene por objetivo la protección frente a los perjuicios imputables a defectos de disponibilidad, de confidencialidad y de integridad.

Por consiguiente, el alcance y contenido de los objetivos de seguridad enunciados en el artículo 9.1 de la Ley Orgánica puede ser interpretado, en principio, como equivalente al alcance y contenido de los conceptos confidencialidad, integridad y disponibilidad: la integridad evita la alteración indebida de los datos personales, la disponibilidad previene de su pérdida y la confidencialidad impide su tratamiento o acceso no autorizados.

Sin embargo, una interpretación del principio de seguridad tan amplia como la que se desprende de este primer análisis podría conducir a incluir en el ámbito de protección de la Ley Orgánica riesgos que difícilmente pueden ser considerados como amenazas al honor o a la intimidad de los

ciudadanos. En particular, la inclusión de la disponibilidad dentro del ámbito de objetivos de seguridad de los datos personales amparados por ella obligaría a contemplar riesgos tales como la destrucción accidental de ficheros o las interrupciones de servicio de los sistemas informáticos, que no pueden concebiblemente poner en peligro los derechos al honor y a la intimidad que constituyen la razón última de la Ley.

Por el contrario, la alteración o pérdida parcial de los datos relativos a una persona pueden, en ciertas circunstancias, conducir a la desfiguración del perfil informativo del individuo, afectando negativamente su reputación o fama y perjudicándole en sus relaciones con los demás.

En consecuencia, si bien los objetivos enunciados por el artículo 9.1 de la Ley Orgánica pueden ser interpretados como sinónimos de los tres principios clásicos de confidencialidad, integridad y disponibilidad, parece claro que su aplicación debe ser contemplada en función de los riesgos concretos que cada situación presenta para el honor e intimidad de las personas cuyos datos están siendo tratados».

Con las presentes bases, se analizaba cómo debían entenderse cada uno de los tres apartados que componían el artículo 9 de la LORTAD:

«En primer lugar, la referencia a medidas técnicas y organizativas viene a consagrar legalmente un principio de gran importancia práctica, como es el carácter multidisciplinar de la seguridad de los sistemas de información. Este principio, recogido en multitud de recomendaciones, estándares y guías de actuación, está también incluido en el citado documento de Directrices de Seguridad de la OCDE, así como en los recientes trabajos de normalización internacional sobre criterios de seguridad (GSSP, Common Criteria), y supone el reconocimiento de que la seguridad no puede ser lograda y mantenida por la simple instalación de dispositivos físicos o lógicos, sino que requiere la consideración de múltiples puntos de vista y la acción concertada de medidas de variada naturaleza, entre las que las relacionadas con los factores humanos no son menos importantes que las tecnológicas.

En segundo lugar, la remisión a un futuro desarrollo reglamentario plantea la cuestión de la exigibilidad de medidas de seguridad hasta tanto no sean aprobados los reglamentos que las determinen.

Con vistas a la actuación de la Agencia en este su primer año de andadura, dos consideraciones

contrapuestas han sido tenidas en cuenta. De un lado, la supeditación de toda exigencia de medidas de seguridad a la aprobación de sus reglamentos de desarrollo podría dejar, por tiempo indefinido, vacío de contenido el principio de seguridad de los datos personales establecido en la Ley y, perdido el soporte de la seguridad, venirse abajo el sistema de garantías de la privacidad diseñado por ésta. De otro, un sistema de seguridad de datos personales no puede ser improvisado y, en consecuencia, la autoridad de control (la Agencia) ha de tener en cuenta la situación general que en materia de seguridad de los sistemas de información predomina en España en el momento de entrar en vigor la Ley, y hacer posible una transición ordenada hacia una nueva situación más acorde con los principios y garantías establecidos por ella.

En tercer lugar, el propio artículo 9.1 establece criterios para determinar cuáles son las medidas a adoptar para garantizar la seguridad de los datos personales requerida por la Ley.

Estos criterios, basados en el principio general de proporcionalidad, son de tres órdenes distintos: el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que dichos datos se encuentran expuestos.

El estado de la tecnología delimita y afecta a las medidas de seguridad que deben ser adoptadas de múltiples formas.

Por una parte, la tecnología determina el ámbito de lo factible en un lugar y momento dados, tanto desde el punto de vista de las amenazas a la seguridad como desde el de las contramedidas que pueden ser adoptadas. En este sentido, puede decirse que la tecnología establece y acota el terreno de juego en que se libra la batalla de la seguridad y su continua evolución introduce nuevas fuentes de riesgo que deben ser previstas, evaluadas y controladas, pero también nuevas posibilidades de protección que deben ser tenidas en cuenta en el diseño de medidas de seguridad. En el año 1994, hemos asistido al surgimiento o expansión de fenómenos tecnológicos que afectaban a uno y otro lado de la balanza de la seguridad: la rápida difusión mundial en el uso comercial o general de la red Internet (por contraposición a su utilización hasta hace poco reducida a ámbitos de investigación o docencia) es un buen ejemplo de cómo la tecnología (o su difusión en la sociedad) puede afectar al equilibrio de la balanza por el lado del riesgo; por otro lado, el surgimiento y evolución de tecnologías para la privacidad, tales como dispositivos físicos o lógicos que facilitan el anonimato en determinadas transacciones electrónicas (algunos tan accesibles y difundidos como el programa Pretty Good Privacy), constituye una muestra de cómo la tecnología también incide en dicho equilibrio por el lado de la protección.

Pero la tecnología es un criterio relevante no sólo porque acota el ámbito de lo factible, sino también porque influye en su coste y su consideración nos conduce al segundo de los criterios establecidos por la Ley: la naturaleza de los datos almacenados. Las medidas de seguridad tienen costes, tanto explícitos (como el tiempo y dinero invertidos en ellas) como implícitos (como pueden ser la agilidad, eficacia o cualesquiera otros objetivos de la organización que han de ser en alguna medida sacrificados para lograr un nivel dado de seguridad).

El principio de proporcionalidad aconseja fijar como objetivo un nivel de seguridad eficiente, esto es, un nivel tal que el coste de las medidas de seguridad sea proporcionado al coste de la "no seguridad", es decir, a los perjuicios de todo tipo que se deriven del riesgo a que están expuestos los datos almacenados. Sobre este equilibrio deseable entre los "costes de la seguridad" y los "costes de la no seguridad" influyen múltiples factores, pero tres de ellos lo hacen de forma decisiva.

El primero, ya considerado, es la tecnología. Las tecnologías de la información no sólo han evolucionado espectacularmente en los últimos años en términos de funcionalidades, sino también de costes. Los efectos combinados de los avances técnicos, la estandarización de componentes y la globalización de los mercados han ocasionado drásticas reducciones de costes en los elementos que integran los actuales sistemas de tratamiento de datos, alterando el equilibrio de la ecuación de costes de la seguridad.

El segundo de estos factores lo constituyen los datos almacenados. Ellos integran el activo a proteger y, por lo tanto, el patrón fundamental para medir lo que es razonable y justo invertir en su seguridad.

Finalmente, y tal como la Ley establece, el riesgo a que los datos personales almacenados o tratados están expuestos es el tercer gran factor a considerar a la hora de determinar cuáles son las medidas de seguridad razonables en cada caso. Si la naturaleza de los datos proporciona la medida del valor a proteger y por lo tanto del perjuicio a evitar, el riesgo a que están expuestos determina la probabilidad de que tal perjuicio se materialice. Por consiguiente, es la combinación de ambos factores (datos a proteger, riesgo a que están expuestos) la que determina el daño esperable que se derivaría de una inadecuada protección, y por lo tanto el nivel de protección exigible.

Podemos concluir, por lo tanto, que la Ley Orgánica proporciona un sistema de objetivos y criterios en materia de seguridad de los datos personales compatible con los principios y criterios generalmente aceptados en el mundo de la seguridad de los sistemas de información y que, aplicado de modo sistemático y complementado en lo necesario con las reglas, técnicas y procedimientos imperantes en dicho mundo, puede permitir discernir la aceptabilidad del conjunto de medidas de protección adoptadas en cada caso, hasta tanto no se plasmen dichos criterios en una regulación detallada como la prevista en los apartados 2 y 3 del artículo 9 de la Ley Orgánica».

Como podemos observar la Agencia Española de Protección de Datos se vio en la necesidad de estableces unos criterios, a todas luces, prácticos que permitiesen la aplicación del principio de seguridad, optando por los criterios básicos del ámbito de la seguridad de la información, al menos, hasta que se hiciese efectivo el ansiado desarrollo reglamentario del principio de seguridad en materia de protección de datos de carácter personal.

2. El principio de seguridad en la Directiva 95/46/CE

El Considerando 46 de la Directiva 95/46/CE dispone:

«Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse».

En virtud de dicho Considerando, la Directiva dedica su octava sección (artículos 16 y 17 de la Directiva) a la confidencialidad y seguridad del tratamiento, disponiendo algunos de los aspectos que ya se regularon en Convenio 108.

En este sentido el artículo 16 establece:

«Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal»

Por su parte, el artículo 17 dispone:

«1.Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.
Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente».

Por tanto, a la necesidad de completar con un desarrollo reglamentario la previsión del artículo 9 de

la LORTAD, se añadía la necesidad de trasponer el contenido establecido en estos artículos por la Directiva. Sin embargo, tal y como apunta Herrán Ortiz, la verdadera novedad de la Directiva respecto al principio de seguridad es la referencia a "tratamientos":

«Tanto el Convenio 108 como la Directiva 95/46/CE -artículo 17- incorporan disposiciones a propósito de la necesidad de adoptar medidas de seguridad del tratamiento de los datos personales, si bien adoptan en su regulación perspectivas bien distintas.
En efecto, si el Convenio 108 únicamente se refiere a las medidas de seguridad de los datos personales, la Directiva además incorpora medidas de seguridad de los tratamientos (cfr. Art. 17.2º), con una regulación más detallada y precisa».

3. El Reglamento de Medidas de Seguridad

La aprobación del Reglamento de Medidas de Seguridad tuvo lugar el 11 de junio de 1999 a través del Real Decreto 994/1999, poco antes de que la LORTAD fuera derogada por la LOPD como resultado de la transposición de la Directiva 95/46/CE a nuestro ordenamiento.

Su exposición de motivos establecía que:

«La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas 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 estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3.h de la Ley Orgánica 5/1992.

El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor».

Del análisis de las medidas de seguridad incluidas en el Reglamento de Medidas de Seguridad se desprende que son similares a las de los estándares internacionales existentes en el momento de su aprobación. No obstante, a diferencia de estos estándares internaciones, que son voluntarios y tienen la consideración de buenas prácticas, las medidas de seguridad exigidas por el Real Decreto 994/1999 si resultaban de obligado cumplimiento para todos los responsables de ficheros que en su actividad trataran datos personales.

4. El principio de seguridad en la LOPD

La aprobación de la Ley Orgánica 15/1999 de Protección de Datos derogó la LORTAD y transpuso el contenido de la Directiva a nuestro ordenamiento. En lo relativo al principio de seguridad, éste fue enunciado en el artículo 9 de la LOPD siendo ambos artículos prácticamente idénticos, siéndo la única diferencia la mención que realiza la LOPD al encargado del tratamiento entre los obligados a la adopción de medidas de seguridad y la extensión del ámbito de aplicación a los ficheros no automatizados.

En este sentido Herrán Ortiz[189] señala que:

189 HERRÁN ORTIZ, A. (2002): *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Dykinson. Madrid. Página 240.

«La primera novedad que presenta esta norma respecto a la legislación anterior es la relativa a la obligación para el "encargado del tratamiento" de adoptar las medidas de seguridad, ello de acuerdo con la configuración jurídica y la importancia que este sujeto adquiere en la LOPD, y a la que se han realizado los oportunos comentarios en el epígrafe anterior.

Luego, además de al responsable del tratamiento, desde la LOPD también obligan al encargado del tratamiento las medidas de seguridad, ello con independencia de que el Reglamento nada establezca a este respecto».

Esta falta de cambio ha sido duramente criticada por la doctrina española. En este sentido Gómez Navajas[190] considera un error que el legislador no hubiese emprendido una reforma en profundidad de la LORTAD, manteniendo en gran parte un contenido que encaja con dificultad con las novedades introducidas por la directiva comunitaria:

«La valoración que merecía la LORTAD, era, en general, negativa. Se trataba de una ley que había defraudado las expectativas de mejora de la protección de los datos de carácter personal que habían ido surgiendo en nuestro país, auspiciadas por la tardanza del legislador y que dio lugar a que se plantearan cuatro recursos de inconstitucionalidad.

Finalmente, la LORTAD fue derogada por la LOPD; de 13 de diciembre de 1999, que pretendía adaptar el Derecho Español a 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.

La necesidad de transponer la directiva 95/46/CE requería una reforma de la LORTAD que podía haber consistido en una revisión de dicha norma y no en una modificación concreta de aspectos afectados por la Directiva».

El primer apartado del artículo 9 LOPD recoge la obligación de garantizar la seguridad de los tratamientos en términos generales, haciendo referencia a las medidas de índole técnica y

190 GÓMEZ NAVAJAS, J. (2005). *La protección de datos personales. Un análisis desde la perspectiva del derecho penal.* Thomson Civitas. Madrid.

organizativa que resulten necesarias. Por su parte, su segundo apartado prohíbe el almacenamiento de datos personales en ficheros que no reúnan las condiciones que reglamentariamente se determinen. Por último, en su apartado tercero, anuncia un régimen específico para los datos especialmente protegidos.

Por último, destacar que parte del artículo 17 de la directiva, fue incluido en el artículo 12 de la LOPD, relativo a los encargos del tratamiento. Aspecto que ha sido resuelto por el Reglamento de desarrollo de la LOPD al incluir entre los artículos dedicados a la seguridad, algunos referentes al encargado del tratamiento.

5. Diferencias con la Seguridad de la Información

A pesar de que el artículo 9 de la LOPD se encuentra inspirado por los principios de seguridad de la información, el ámbito de aplicación de la normativa de protección de datos es más *limitado*.

El concepto «*Seguridad de la información*» es más amplio pudiendo definirse como «*la protección y preservación de un conjunto organizado de datos procesados, independientemente del medio donde estos se encontraren*».

Para poder comprender la relación entre este concepto y el principio de seguridad, podemos apoyarnos en la interpretación realizada en su día por la Agencia Española de Protección de Datos. Con anterioridad a la aprobación del Real Decreto 994/1999, la Agencia Española de Protección de Datos organizó una conferencia sobre "Seguridad, Privacidad y Protección de Datos" los días 30 de noviembre y 1 de diciembre de 1995 en la cual Juan José Martín-Casallo, propugnó la restricción del ámbito de las medidas de seguridad:

«(…) No toda sanción o incumplimiento de medidas de seguridad determina un ataque directo o indirecto a la privacidad por lo que solamente aquel que ponga en peligro dicho bien jurídico protegido deberá ser atajado por afectar a la confidencialidad en el tratamiento del dato personal.

En este aspecto no parece ilógico afirmar que en la referida enumeración se contemplan supuestos en los que prima con carácter exclusivo la seguridad del sistema informático con desaparición del concepto de intimidad. Así, la pérdida o destrucción -sobre todo la accidental- de sistemas informáticos cuando no va seguida, como ocurrirá en la mayoría de los supuestos, de un acceso

ilícito al tratamiento por parte de un tercero, no sólo no pondrá en peligro la privacidad o la confidencialidad del dato, sino que en términos estrictos supondrá un reforzamiento de la misma.

La desvinculación entre medida de seguridad y privacidad aún cobra una mayor importancia cuando nuestra Ley Orgánica (artículo 9.1) incluye no sólo a la acción humana sino también al medio físico o natural como agentes capaces de ocasionar la pérdida o destrucción del tratamiento informatizado, aludiendo por tanto al caso fortuito o a la fuerza mayor que son causas excluyentes de la culpabilidad necesaria para la imposición de una sanción».

En lo relativo al principio de seguridad establecido por la LOPD, para que se aprecie una vulneración de las medidas de seguridad sancionable, esta habrá de fundamentarse en un ataque contra el bien jurídico protegido por esta norma e implicar tratamiento de datos personales. No obstante, debemos resaltar que el Título VIII del Reglamento de desarrollo de la LOPD es la única norma que contiene previsiones relativas a seguridad de cumplimiento obligatorio para las empresas, sin que esto implique, necesariamente, que no deba tenerse en cuenta el concepto de Seguridad de la Información ya que en la actualidad existen numerosos estándares que son una referencia y que pueden servir como apoyo o complemento a las obligaciones contenidas en la LOPD.

II. EL PRINCIPIO DE SEGURIDAD EN EL REGLAMENTO DE DESARROLLO DE LA LOPD.

1. Introducción

El Título VIII del Reglamento de desarrollo de la LOPD, titulado «De las medidas de seguridad en el tratamiento de datos de carácter personal», se estructura de la siguiente forma:

Capítulo I. Disposiciones Generales: Este capítulo recoge la regulación de los aspectos básicos, del desarrollo reglamentario del principio de seguridad. Se regulan, entre otros, los siguientes aspectos:

Alcance de la regulación del principio de seguridad: El artículo 79 Reglamento de desarrollo de la LOPD se limita a establecer que serán los responsables de los tratamientos o los ficheros y los encargados del tratamiento los que deberán implantar las medidas de seguridad con

independencia de cuál sea su sistema de tratamiento.

Niveles de seguridad: La atribución de los niveles de seguridad a los datos de carácter personal es prácticamente idéntica a la que ya realizaba el Reglamento de Medidas de Seguridad.

Prestaciones de servicios: Se regulan las obligaciones relacionadas con el principio de seguridad en los encargos del tratamiento.

Capítulo II. El Documento de Seguridad: Se dedica al desarrollo de las obligaciones relacionadas con el Documento de Seguridad así como cual es el contenido del mismo.

2. Niveles de seguridad

2.1 Introducción

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, 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 establecía, en su Considerando 46:

«(46) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse»

Como ya hemos dicho anteriormente, estas consideraciones tuvieron su reflejo en el artículo 17.2 del mismo texto, de acuerdo con el cual:

«(…) Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente

el tratamiento y con la naturaleza de los datos que deban protegerse».

Por su parte, el artículo 9 LOPD regula la aplicación de este principio de seguridad de los datos estableciendo que el responsable del fichero y, en su caso, el encargado de tratamiento, deberán 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 estableciendo para ello tres criterios: el estado de la tecnología, los riesgos a los que se encuentran expuestos los datos personales almacenados y la naturaleza de dichos datos.

En este sentido, la naturaleza de los datos es uno de los criterios fijados por la norma para el establecimiento de los tres niveles de seguridad en los que se clasifican las medidas de seguridad. Por naturaleza de los datos nos referimos al tipo de información que podrá obtenerse del tratamiento de los datos y a la forma en que la misma puede afectar a los derechos y libertades del interesado, lo que justifica en determinados casos el establecimiento de un nivel especial de protección. Corresponde, por tanto, analizar como el Reglamento de Medidas de Seguridad y, posteriormente, el Reglamento de desarrollo de la LOPD ha estructurado los niveles de protección en base a la naturaleza de los datos personales.

2.2 Niveles de seguridad

Los niveles de seguridad, se encontraban ya regulados por los artículos 3 y 4 del Reglamento de Medidas de Seguridad, cuyo contenido exponemos a continuación:

*«**Artículo 3. Niveles de seguridad.***
1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información».

*"**Artículo 4. Aplicación de los niveles de seguridad.***
1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes».

Por tanto, en virtud de los citados artículos, todos aquellos ficheros que contenían datos de carácter personal debían aplicar:

1. Medidas de nivel básico: En todo caso y como requisito previo para poder llevar a cabo cualquier tratamiento de datos personales. Sobre la base de estas medidas los restantes niveles de seguridad debían ser aplicados de forma acumulativa; es decir, que al nivel de seguridad medio eran de aplicación las medidas de seguridad del Nivel Básico y las medidas de nivel alto abarcaban, a su vez, las de nivel medio y básico.
2. Medidas de carácter general. Además se preveían una serie de medidas de carácter general que, con independencia del nivel de seguridad aplicable, cualquier tratamiento de datos personales debía incluir en caso de que se dieran algunas de las circunstancias previstas. Se encontraban recogidos en los artículos 5 a 7 del Reglamento de Medidas de Seguridad que si bien resultaban de aplicación a todos los ficheros, solo eran de aplicación en las siguientes circunstancias:
    a. Accesos a datos a través de redes de comunicaciones.
    b. Ejecución de tratamientos fuera de los locales de ubicación del fichero.
    c. Creación y tratamiento de ficheros de carácter temporal.
    d. Medidas de nivel básico

3. Medidas de nivel medio: Su aplicación se preveía en el caso de ficheros relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos relativos a la solvencia patrimonial y el crédito de las personas y al cumplimiento o incumplimiento de sus obligaciones dinerarias. En este sentido debemos citar la interpretación de la Agencia Española de Protección de Datos sobre estos los conceptos y que deben interpretarse de la siguiente forma:

a. Datos de Hacienda Pública: Ficheros cuya titularidad corresponda a la Hacienda Pública, debiendo entenderse por tanto, aquellos ficheros cuyo responsable sea una Administración Pública que ostente potestades en materia tributaria.

b. Servicios financieros: Se incluyen las actividades de intermediación financiera, la intermediación monetaria, las actividades relacionadas con la Banca Central, Bancos, Cajas y Cooperativas, las actividades de arrendamiento financiero, las llevadas a cabo por Sociedades de crédito hipotecario, entidades de financiación, Sociedades mediadoras en el mercado de dinero y el Instituto de Crédito Oficial (ICO), así como las efectuadas por Instituciones de inversión colectiva de carácter financiero, Sociedades y fondos de capital riesgo y otras sociedades de inversión en activos financieros.
Son también servicios financieros los relacionados con la Administración de mercados financieros y las actividades llevadas a cabo por sociedades de valores, sociedades de garantía recíproca y de reafianzamiento, sociedades de tasación, casas de cambio, fondos de garantía de depósito y sus sociedades gestoras.
Adicionalmente, la Clasificación Nacional de Actividades Económicas incluye dentro de los servicios de intermediación financiera los relacionados con seguros de vida, los planes de pensiones y los seguros de daños y el reaseguro. También se consideran actividades de intermediación financiera las efectuadas por agentes y corredores de seguros e intermediarios de seguros.

c. Datos que permitan una evaluación de la personalidad del individuo: Antes de comentar el nivel de seguridad alto es necesario mencionar, siquiera brevemente, otra categoría que alude al régimen previsto para el caso de que el tratamiento incluya un conjunto de datos personales suficientes que permitan obtener una evaluación de la personalidad del individuo. Para estos casos el Reglamento de Medidas de Seguridad un nivel intermedio entre el nivel básico y el medio siendo necesario aplicar el nivel de seguridad medio así como algunas de las medidas de seguridad del nivel medio. A través de este sistema se admitía la existencia de tratamientos que se encontraban en la frontera entre los de nivel básico y medio.
En relación al concepto de tratamiento que permita obtener una evaluación de la personalidad del individuo, se trata de un concepto jurídico indeterminado que responde al riesgo que

pueden presentar algunos datos que si bien individualmente revelan aspectos parciales del titular de los mismos, cuando se fusionan en un tratamiento orientado a este fin, pueden llegar a ofrecer un perfil concreto del individuo. En este sentido Martínez Sánchez[191] sostiene que: «*En mi opinión, la aplicación de las precisiones contenidas en el artículo 4.4 Reglamento de Medidas de Seguridad se producirá cuando se sumen las dos circunstancias, por un lado, que se almacenen en fichero un número de facetas suficientes del individuo y por otro lado, que se realicen tratamientos que permitan acceder a un conocimiento de actitudes, hechos o pautas de comportamiento que, sin duda alguna, podrían determinar el perfil de las personas que pertenece a su esfera privada.*

En todo caso, conviene puntualizar que, para obtener estos perfiles, sería necesario el consentimiento de los interesados en los términos previstos en el artículo 4.2 de la LOPD, toda vez que los datos de carácter personal objeto de tratamientos , no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos».

4. Medidas de nivel alto: Era de aplicación a todos aquellos ficheros que contengan datos personales que revelen la ideología, afiliación sindical, religión y creencias o que hagan referencia al origen racial, a la salud y a la vida sexual de las personas así como a los que contengan datos recabados con fines policiales sin consentimiento de las personas afectadas. La presente clasificación representaba una importante fuente de obligaciones para los responsables de los ficheros. Uno de los casos más ejemplificativos era la gestión de la nómina de los empleados de una entidad y que en base a lo estipulado por el Reglamento de Medidas de Seguridad, era necesario implantar medidas de nivel alto para proceder a su tratamiento. La presente situación obligó a que la Agencia Española de Protección de Datos se viese obligada a interpretar diversos supuestos para calificar los tratamientos con uno u otro nivel y que finalmente ha sido resuelta en la redacción del Reglamento de desarrollo de la LOPD, que ha enfocado el tema con una mayor flexibilidad.

Una vez analizados los niveles de seguridad desde el punto de vista del Reglamento de Medidas de Seguridad corresponde analizar ahora la visión de dichos niveles en el Reglamento de desarrollo de la LOPD y que se encuentran regulados en sus artículos 80 y 81:

«***Artículo 80. Niveles de seguridad.***

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles:

191 MARTÍNEZ SANCHEZ, M. (2001): *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*. Universidad Pontificia de Comillas. XIV Encuentros sobre Informática y Derecho 2000-2001. Editorial Aranzadi. Madrid. Página 74.

básico, medio y alto».

*«**Artículo 81. Aplicación de los niveles de seguridad.***

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los relativos a la comisión de infracciones administrativas o penales

b. Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e. Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c. Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b. Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

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

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación

en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad».

En relación a los ficheros de nivel medio, podemos destacar tres aspectos novedosos en relación a la anterior regulación:

- Son de aplicación a los ficheros o tratamientos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.
- También se aplica este nivel a aquéllos ficheros que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
- Asimismo también es de aplicación este nivel a aquellos tratamientos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

En relación a los ficheros de nivel alto las principales novedades del Reglamento de medidas de seguridad son las siguientes:

- El reconocimiento de los ficheros que contengan datos derivados de actos de violencia de género.
- El tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas, para los que se establece un régimen especial.

En relación a las novedades se hace necesario destacar que una de ellas es que el establecimiento de los niveles de seguridad ya no se realiza únicamente en función de la naturaleza de la información tratada, tal y como sucedía con el Reglamento de Medidas de Seguridad. En este sentido el Reglamento de desarrollo de la LOPD tiene en cuenta diferentes factores para esta clasificación: El tipo y naturaleza de los datos contenidos, el tipo de actividad y el objeto social del responsable del fichero o la naturaleza pública o privada del mismo.

Por otro lado, el artículo 81.6 Reglamento de desarrollo de la LOPD es uno de los preceptos más controvertidos de este Reglamento lo que ha forzado a la Agencia Española de Protección de Datos

ha realizar una interpretación del mismo. De acuerdo con este artículo, las medidas de seguridad aplicadas a los tratamientos de datos relativos a la salud o al grado de discapacidad cuando el mismo se realice con motivo del cumplimiento de deberes públicos, podrán ser de nivel básico. Por tanto, el presente artículo modifica la calificación de nivel alto de los ficheros de nóminas que mantienen todas las entidades, eliminando una obligación altamente gravosa.

En este sentido el Informe 91/2008[192] de la Agencia Española de Protección de Datos interpreta el contenido del artículo 81 en relación con los ficheros de nóminas y Seguridad Social:

«La consulta plantea, sí el Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la Ley Orgánica 15/1999, de 13 de enero de Protección de Datos de Carácter Personal, modifica el nivel de seguridad que debe aplicarse a los ficheros de nóminas y de la Tesorería General de la Seguridad Social.

En todo caso, debe indicarse como cuestión previa que según la disposición final segunda del mencionado Real Decreto, dicha norma no entrará en vigor hasta transcurridos tres meses desde su publicación en el Boletín Oficial del Estado, habiendo tenido la misma lugar el 19 de enero de 2008.

No obstante, pasaremos analizar las cuestiones suscitadas en la consulta.

En primer lugar respecto a las medidas de seguridad que debe de aplicarse al fichero de nóminas, el artículo 81.6 del Real Decreto 1720/2007 señala que "6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos."

Por ello, los datos relativos a la minusvalía siguen siendo datos relativos a la salud, lo único que se permite es adoptar medidas de seguridad de nivel básico en cuanto a dicho dato se encuentre afectado o vinculado al cumplimiento de deberes públicos, como sería el supuesto del fichero de nóminas en el que aparezca un porcentaje de minusvalía para calcular el nivel de retención aplicable en nómina, conforme a lo previsto en el artículo 103.1 del Real Decreto Legislativo

192 Agencia Española de Protección de Datos (2008). Informe jurídico 0091-2008 sobre medidas de seguridad en ficheros de la Seguridad Social.

3/2004, de 5 de marzo por el que se aprueba el Texto Refundido del Impuesto sobre la Renta de las Personas Físicas. En consecuencia si el dato de minusvalía se tratará para cuestiones que no constituyan el cumplimiento de deberes públicos, sí deberán de adaptarse mediadas de seguridad de nivel alto.

Por último en cuanto a los Ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social el artículo 81.2 señala que "Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: . Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social"

Por ende, sólo los ficheros comunes de las Entidades Gestoras de la Seguridad Social deberán adoptar las medidas de seguridad de nivel medio, por tanto, para el caso de que dicha entidad disponga de ficheros en los que se recojan datos especialmente protegidos, o cuando se traten datos de carácter personal, de los previstos en el artículo 81.3 del Real Decreto 1720/2007 como son:

"a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.", en éstos deberán implantar las medidas de seguridad de nivel alto».

Otro punto novedoso corresponde a los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas. Nos encontramos aquí ante el caso específico de los ficheros de los que son responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y localización y que en todo caso deberán aplicar las medidas de nivel básico, las de nivel medio así como la medida de seguridad de nivel alto relativa al registro de control de accesos.

Asimismo otra novedad importante tiene que ver con los ficheros que contengan datos para la evaluación de la personalidad. En este sentido el Reglamento de desarrollo de la LOPD establece una mejora en relación a su predecesora ya que ahora no se habla de la necesidad de contar con *«datos suficientes para poder obtener una evaluación de la personalidad»* sino que exige que efectivamente el fichero contenga datos referentes a *«características o personalidad de los ciudadanos»* y que estos datos permitan a su vez *«evaluar la personalidad y comportamiento»* de los mismos. No obstante, el contenido del artículo 81.2 f) no es excesivamente claro y, por tanto, queda sujeto a valoraciones e interpretaciones dispares. En este sentido, debemos acudir al artículo 36.1 RDLOPD que, en relación con el derecho de oposición establece qué puede suponer una evaluación de personalidad. En concreto se refiere a ellas como aquellas actividades encaminadas a *«evaluar el rendimiento laboral, crédito, fiabilidad o conducta»* del individuo.

3. Encargos del tratamiento

3.1 El encargado de tratamiento

La aprobación del nuevo Reglamento de desarrollo de la LOPD ha significado el reconocimiento de su importancia en relación con el cumplimiento del principio de seguridad. El artículo 82 aporta al marco normativo español un aspecto que ni la LOPD ni el Reglamento de Medidas de Seguridad habían tenido en cuenta. No debemos olvidar que la LOPD, cuando regula esta figura lo hace de forma completamente independiente del cumplimiento del principio de seguridad, situación que cambia radicalmente en el artículo 82 Reglamento de desarrollo de la LOPD que, pone en relación los accesos por cuenta de terceros con el principio de seguridad, entrando a regular este tipo de accesos en los que se deberá compatibilizar la figura del Encargado de Tratamiento con el cumplimiento del artículo 9 LOPD.

El enfoque aportado por el Reglamento de desarrollo de la LOPD en este sentido es doble:

- Acceso a datos contenidos en recursos y sistemas del responsable del fichero. En primer lugar se regula el supuesto de que los datos accedidos se mantengan en los locales y recursos del responsable del fichero.
  En este caso, el Reglamento se limita aquí a exigir que los accesos estén adecuadamente controlados disponiendo el artículo 82.1 que:

«*1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el Documento de Seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento*».

Se regula por lo tanto la obligación de incluir en el Documento de Seguridad los accesos por cuenta de terceros autorizados y las circunstancias en los que los mismos se producirán.

Cabe también la posibilidad de que el servicio se preste desde las instalaciones del encargado de tratamiento, pero que, de acuerdo a lo establecido por las partes, este acceso no implique el almacenamiento en recursos o sistemas del encargado de tratamiento. En este caso, el Reglamento de desarrollo de la LOPD establece:

«*Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el Documento de Seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento*».

- Régimen de trabajo fuera de los locales del Encargado de Tratamiento. Existe la posibilidad de que el acceso implique el almacenamiento de los datos utilizando recursos del encargado de tratamiento. En este supuesto, el Reglamento de desarrollo se centra en garantizar el cumplimiento de las medidas de seguridad por el responsable y prevé la delegación de la responsabilidad de elaborar y mantener el Documento de Seguridad en el encargado de tratamiento. Tal y como establece el artículo 82.2:

  "2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un Documento de Seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento».

  La presente obligación se completa con lo previsto por el artículo 88.6 del Reglamento para aquellos casos en los que el tratamiento se realice exclusivamente en los sistemas del encargado:

  «*6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado*

la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.
En tal caso, se atenderá al Documento de Seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento».

3.2 Contratación del encargo del tratamiento

El compromiso por parte del encargado del tratamiento de implementar y cumplir en sus instalaciones las medidas de seguridad correspondientes deberá ser una de las cláusulas fundamentales de los contratos que firme con el responsable del fichero. En este sentido, resulta recomendable establecer cláusulas en las que se establezcan indemnizaciones que pagará el encargado del tratamiento al responsable del fichero en caso de incumplimiento doloso o negligente de las medidas de seguridad. No obstante existen también otra serie de cuestiones a tener en cuenta a la hora de redactar un contrato de encargo del tratamiento en los términos del artículo 12 de la LOPD:

- Presentación de las resoluciones de la Agencia Española de Protección de Datos por las que se inscriben en el Registro General de Protección de Datos los ficheros titularidad del encargado del tratamiento.
- Presentación del documento de seguridad.
- Nombramiento de un responsable de seguridad o coordinador interno que pueda actuar de interlocutor en relación a las dudas.
- Presentación del último informe bienal de auditoría de medidas de seguridad.
- Cláusulas de confidencialidad en los contratos de trabajo firmados por sus empleados.

Estas consideraciones deberán tenerse en cuenta no solo para los nuevos contratos de prestación de servicios, sino que será necesario llevar a cabo una revisión de los contratos ya suscritos para su adecuación al Reglamento de desarrollo de la LOPD, para aquellos encargos del tratamiento celebrados con anterioridad a la entrada en vigor del Reglamento de Desarrollo de la LOPD.

3.3 Encargos sin acceso a datos personales

Existe la posibilidad de que existan prestaciones de servicios que no conlleven un acceso a datos de carácter personal y que incluso se encuentran previstos en el artículo 83 de la LOPD que establece:

«El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio».

En este sentido podemos observar que la primera obligación se trata de una obligación ya impuesta por el propio artículo 91 del Reglamento de desarrollo de la LOPD sobre control de accesos. No obstante, el responsable del fichero deberá implantar medidas de seguridad específicas dirigidas a prestadores de servicios sin acceso a datos. En segundo lugar, en los contratos celebrados con los prestadores sin acceso a datos, habrá de incluirse una cláusula que obligue al prestador del servicio a informar a todos sus empleados de la prohibición de acceder a cualquier soporte que contenga datos personales así como el acceso a los recursos que contenga el sistema de información. Cualquier acceso accidental será inmediatamente comunicado al responsable del fichero y obligará al prestador y a sus trabajadores al secreto profesional respecto a la información de la que se haya tenido conocimiento.

4. El Documento de seguridad

El Reglamento de Medidas de Seguridad regulaba el documento de seguridad en sus artículos 8 y 15, mientras que por su parte el Reglamento de Desarrollo de la LOP lo recoge en un único artículo, el 88.

En este sentido, el Reglamento de Medidas de Seguridad reglaba, por un lado, el Documento de Seguridad para ficheros a los que son de aplicación las medidas de seguridad de nivel básico y, por otro, las obligaciones de este documento en el caso de que resultaran aplicables las medidas de seguridad de nivel medio u alto. De esta forma el artículo 8.1 disponía:

«El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información».

Por su parte, el artículo 88.1 del Reglamento de desarrollo de la LOPD dispone:

«El responsable del fichero o tratamiento elaborará un Documento de Seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información».

Al comparar ambos artículos es inevitable observar algunas diferencias:

- Ambos señalan que será el responsable del fichero el que elabore el documento de seguridad, pero el Reglamento de Medidas de Seguridad establecía que además lo implantará.
- El Reglamento de desarrollo de la LOPD añade que el Documento de Seguridad debe recoger las medidas de índole técnica y organizativa acordes a la normativa vigente.
- El nuevo Reglamento de desarrollo suprime cualquier referencia a la palabra automatizado, ya que este es de aplicación para ficheros y tratamientos tanto automatizados como no automatizados. Además, señala que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

El Reglamento de desarrollo de la LOPD establece en el segundo apartado del artículo 88, cuales son las formas de elaborar el documento de seguridad:

- El Documento de Seguridad podrá ser:
  - Único y comprensivo para todos los ficheros o tratamientos o,
  - Individualizado para cada fichero o tratamiento.
- Podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según:
  - El sistema de tratamiento utilizado para su organización, o
  - Atendiendo a criterios organizativos del responsable
- En todo caso, tendrá el carácter de documento interno de la organización.
-

Según lo establecido en el Reglamento de desarrollo de la LOPD, el Documento de Seguridad deberá contener, de forma necesaria:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por el reglamento.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

5. Definiciones

Antes de adentrarnos en el estudio de las medidas de seguridad, debemos realizar un inciso para examinar las definiciones contenidas en el artículo 5.2 Reglamento de desarrollo de la LOPD y que es necesario conocer antes de proceder al estudio de las ya citadas medidas de seguridad.

El artículo 5.2 del Reglamento de desarrollo establece las siguientes definiciones:

- **Accesos autorizados:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad. En este sentido el Reglamento de desarrollo establece una segunda frase aclaratoria, con respecto al Reglamento de medidas de seguridad, que como señala Davara: «*viene a cubrir el anterior defecto del Reglamento de Medidas de Seguridad, que presentaba problemas operativos cuando funciones que tenía el responsable del fichero y que no podía delegar las tenía que ejecutar, como es natural, una persona determinada o,*

en otro caso, reunirse el propio responsable del fichero (el Consejo de Administración de la entidad, por poner un ejemplo) cada vez que había que autorizar una de estas funciones».

- **Autenticación:** Procedimiento de comprobación de la identidad de un usuario.
- **Contraseña:** Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.
- **Control de acceso:** Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- **Identificación:** Procedimiento de reconocimiento de la identidad de un usuario.
- **Copia de respaldo:** Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- **Documento:** Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
- **Soporte:** Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
- **Transmisión de documentos:** Cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo. El presente concepto constituye una de las novedades más destacadas del nuevo reglamento de desarrollo de la LOPD. Sin embargo, resulta desafortunado recoger este término en el catálogo de definiciones teniendo en cuenta que en éste también figura el concepto de *"soporte"*. En este sentido puede entenderse que el documento es un archivo que puede ser tanto físico como lógico, frente al soporte que, como indica la definición, es un objeto físico.
- **Recurso:** Cualquier parte componente de un sistema de información.
- **Sistema de información:** Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Ficheros temporales:** Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento. En este sentido conviene matizar que los ficheros temporales pueden ser automatizados o en papel.
- **Incidencia:** Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos. Generalmente se identifica incidencia con un problema informático, pero en el contexto de las medidas de seguridad del Reglamento de desarrollo de la LOPD puede referirse también a aspectos de seguridad física.
- **Perfil de usuario:** Accesos autorizados a un grupo de usuarios.
- **Usuario:** Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin

identificación de un usuario físico. El concepto "*perfil de usuario*", que proveniente de la Informática, hace referencia a los privilegios otorgados a cada usuario en el sistema de información, y debe entenderse aplicada también a ficheros manuales.

- **Responsable de seguridad:** Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. El nombramiento de un responsable de seguridad resulta obligatorio para los niveles medio y alto y debe constar en el Documento de Seguridad con independencia de que el tratamiento sea automatizado o no automatizado.
- **Sistema de tratamiento:** Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

III. MEDIDAS DE SEGURIDAD

Las medidas de seguridad establecidas por el Reglamento de desarrollo de la LOPD son claras herederas de las contenidas en el Reglamento de Medidas de Seguridad, con algunos matices o modificaciones realizados en base a la experiencia y la práctica de los años en los que estuvo en vigor el Reglamento de Medidas de Seguridad.

Debemos partir de la base de que las medidas de seguridad es el núcleo de las obligaciones para el responsable del fichero y, en su caso, para el encargado de tratamiento. No debemos olvidar que el reglamento de desarrollo de la LOPD exige la aplicación de controles, procedimientos y medidas a todos los tratamientos de datos personales, lo que implicará actuar en ámbitos organizativos y técnicos así como establecer políticas y protocolos de actuación que garanticen el cumplimiento de las obligaciones recogidas por la norma.

Por lo tanto, es el momento de centrarnos en el análisis y estudio de las medidas de seguridad establecidas en el Reglamento de desarrollo de la LOPD.

1. Antecedentes

Debemos partir de la base de la Sentencia 292/2000, de 30 de noviembre, que se pronunciaba de la siguiente forma:

«el Tribunal Constitucional, en las SSTC citadas, ya ha señalado que respetadas esas exigencias y garantizada la seguridad de los datos, resulta legítimo el tratamiento de datos personales y su posterior comunicación».

Parece claro pues que si no existe un cumplimiento adecuado de las medidas de seguridad establecidas en la normativa, no resulta legítimo ningún tratamiento de datos de carácter personal. Tanto la LORTAD como la LOPD recogen esta obligación y, en este sentido, el artículo 9.2 de la LOPD establece que:

«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».

Articulado que no hace sino seguir las estipulaciones de la Directiva 95/46/CE del Parlamento Europeo y del Consejo cuyo Considerando 25 establece:

«(25) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos -obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control v las circunstancias en las que se puede efectuar el 'tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias».

Lo expresado en el Considerando 25 se debe poner en relación con el Considerando 46 que exigía la implantación de medidas técnicas y de organización apropiadas, tanto en el momento de concepción del sistema de tratamiento, como en su aplicación sobre los datos, que garantizaran un nivel de seguridad adecuado en función del estado de la técnica y del coste de su aplicación en relación con los riesgos en presencia:

«(46) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado;

Que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas;

Que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse».

Como podemos observar, el principio de seguridad no representa un principio más dentro de la regulación de la protección de datos, sino que nos encontramos en presencia de un auténtico condicionante previo para el tratamiento de los datos de carácter personal, hasta tal punto, que en el momento de cumplir con el requisito de declarar el tratamiento ante la Autoridad de Control, el responsable del fichero, deberá indicar qué nivel de protección será de aplicación al nuevo tratamiento.

En lo relativo a las medidas a implantar, la Directiva, en su artículo 17**,** desarrolla lo previsto en los Considerandos 25 y 46, enunciando la obligación de los Estados miembros de establecer las obligaciones que permitan aplicar el principio de seguridad y estableciendo la obligación del responsable del tratamiento de aplicar las medidas previstas en cada caso, previendo la posibilidad de que estas obligaciones sean cumplidas por un encargado de tratamiento en el que el responsable delegue:

*«**Artículo 17. Seguridad del tratamiento***

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el

acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.
4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente».

Podemos observar que la Directiva no concreta cuales deben ser las medidas de seguridad que los Estados miembros exigirán en cada caso, estableciendo únicamente que las mismas garanticen un nivel de seguridad adecuado. El artículo 9 de la LOPD recoge esta obligación establecida por la norma comunitaria disponiendo que el responsable del fichero y, en su caso, el encargado de tratamiento, deberán 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 los que están expuestos.

El Reglamento de Desarrollo de la LOPD, que deroga el Reglamento de Medidas de Seguridad, regula en detalle la aplicación del principio de seguridad al que dedica su Título VIII. El Reglamento de Desarrollo de la LOPD parte de un análisis de los puntos débiles contenidos en el Reglamento de Medidas de Seguridad y añade la adaptación de la regulación en aspectos como la atribución de los niveles de seguridad y la fijación y revisión, en su caso, de las medidas de

seguridad que corresponda adoptar en cada caso.

En este sentido es remarcable la regulación de un conjunto de medidas destinadas a los ficheros y tratamientos no automatizados que con anterioridad no habían sido desarrollados y que ahora permiten un marco claro de actuación respecto de los mismos.

2. Medidas de seguridad de nivel básico en los ficheros automatizados

Se regulan en los artículos 89 a 94 del Reglamento de desarrollo de la LOPD, siendo necesario que las presentes medidas deban implantarse en cualquier tratamiento de datos de carácter personal, con independencia de la clasificación que corresponda a los datos en cuestión. Analicemos, por tanto, cada una de estas medidas de seguridad.

2.1 Funciones y obligaciones del personal

Se encuentra regulada en el artículo 89 del Reglamento de desarrollo de la LOPD que dispone:

«1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento».

Corresponde al responsable del tratamiento establecer los medios para que el personal conozca las funciones que debe cumplir con respecto a la protección de datos de carácter personal así como las consecuencias derivadas de su incumplimiento. La presente medida no es meramente formal siendo una de las más importantes. No podemos olvidar que ninguna política de protección de datos será

eficiente si no se lleva a cabo en la organización una labor previa de asignación de tareas bien definida así como una correcta comunicación a y entre todos los miembros de la misma.

Una vez definidas, deben establecerse medidas para informar adecuadamente al personal de cuáles son sus funciones y obligaciones respecto a los tratamientos de datos personales. Para ello debe utilizarse un lenguaje comprensible que garantice que la totalidad del personal comprende la responsabilidad y el riesgo asumido al tratar con este tipo de información.

En relación a los medios a utilizar para esta comunicación, puede utilizarse cualquiera que el Responsable del Tratamiento tenga disponible y resulte adecuado para esta finalidad: notificación, escrito, al inicio del programa -como pantalla de paso obligatorio-, a través de la Intranet corporativa...

El personal afectado por esta obligación puede clasificarse de la siguiente forma:

- **Administradores del sistema**, encargados de administrar o mantener el entorno operativo de los ficheros.
- **Usuarios** o personal que utiliza los datos personales contenidos en los ficheros.
- **En su caso, un Responsable de Seguridad** cuyas funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el Responsable del Tratamiento, sin que esto suponga en ningún caso una delegación de la responsabilidad que, en todo caso, corresponde siempre a el Responsable.

En este punto cabe plantearse si el contenido del artículo 89 del Reglamento de desarrollo de la LOPD incluye la obligación de identificar a las personas físicas a las que se asignan las funciones y obligaciones en concreto. Esta duda se planteaba en relación al contenido del artículo 11 del ya derogado Reglamento de Medidas de Seguridad que obligaba al responsable del fichero a elaborar y mantener una relación actualizada de usuarios con acceso autorizado al sistema de información en relación con el establecimiento de procedimientos de identificación y autenticación para dicho acceso. En este sentido, y respecto al concepto de "*usuario*", este fue determinado en su día por la Agencia Española de Protección de Datos en un Informe emitido en 1999:

«Se plantean reiteradamente cuestiones referentes al concepto que ha de darse a las referencias efectuadas por los artículos 9 y 11 del Reglamento, a las expresiones "usuarios" y "personal". En

particular, si es posible cumplir con lo establecido en estos preceptos mediante una invocación general del departamento o unidad en que el personal ejerza sus funciones.

El artículo 9 del Reglamento se refiere a la necesaria documentación y definición de las funciones y obligaciones atribuidas a cada una de las personas con acceso a los datos de carácter personal, añadiendo el apartado segundo que "el responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
Por su parte, en cuanto a lo establecido en el artículo 11, se exige al responsable del fichero la existencia de una relación actualizada de usuarios que tengan acceso autorizado al sistema de información. En este sentido el artículo 2.2 del Reglamento define al usuario como sujeto o proceso autorizado para acceder a datos o recursos. Del tenor de lo dispuesto en ambos artículos, parece deducirse que será indispensable que las obligaciones impuestas en ambos preceptos hagan referencia a las personas físicas con acceso a los datos o que ostenten la condición de usuarios de los mismos.

Esta referencia, en virtud de lo indicado en el artículo 2.2, ya citado, podrá efectuarse bien mediante la plena identificación de la persona usuaria de los datos o bien mediante la indicación de las circunstancias concurrentes en la misma, como por ejemplo el puesto de trabajo desempeñado, de forma que sea posible conocer en cada momento la persona concreta que puede acceder a los datos por referencia a esas circunstancias.

Ello permite diferenciar las obligaciones de identificación impuestas en los niveles de seguridad básico y medio, toda vez que respecto de este último el artículo 18 impone "la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información».

La Agencia Española de Protección de Datos aclaraba así este extremo y dicha aclaración ha sido incluida en el Reglamento de desarrollo de la LOPD ya que en su artículo 89 se habla tanto de "*usuarios*" como de "*perfiles de usuarios*", definiendo estos últimos como "*accesos autorizados a un grupo de usuarios*".

Por último, es necesario destacar que las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a datos personales deberán estar claramente definidos y documentadas en el documento de seguridad, debiendo también definirse las funciones de control o

autorizaciones delegadas por el responsable del fichero o tratamiento. Dentro de estas obligaciones y funciones del personal, señala el Reglamento de desarrollo de la LOPD la obligación del responsable del fichero de que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. De acuerdo con esta obligación, deberán ponerse los medios para el establecimiento de los procedimientos internos necesarios para poder acreditar el cumplimiento de esta obligación destinada a que dicha comunicación y conocimiento por parte del personal, sea efectiva.

2.2 Registro de incidencias

La presente medida de seguridad se encuentra regulada en el artículo 90 del Reglamento de Desarrollo de la LOPD:

«Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas».

Tal y como establece el artículo 5.2 del Reglamento de desarrollo de la LOPD, se entiende por "*incidencia*" cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos. La principal novedad en este punto es la introducción de la obligación de hacer constar en el registro, las medidas correctoras aplicadas en el caso de producirse una incidencia, quedando por lo tanto el contenido de dicho registro fijado en los siguientes conceptos:

- **Tipo de incidencia.** Es conveniente fijar, en el procedimiento de gestión, que tipo de eventos tendrán la consideración de "*incidencia*".
- **Momento en el que se ha producido.** Hablamos de "*el momento en que se ha producido, o en su caso detectado*", habilitando al responsable a registrar el momento de identificación de la incidencia, en caso de que no sea posible determinar el momento en el que la misma se produjo.
- **Persona que realiza la notificación.**
- **Persona a la que se comunica la notificación.**

- **Efectos** derivados de la incidencia para los datos personales gestionados por la organización.
- **Medidas correctoras aplicadas.**

En lo relativo a la gestión del registro de incidencias esta se llevará a cabo mediante procedimientos manuales o informáticos, siendo necesario indicar dicho procedimiento en el documento de seguridad y, en caso de gestión automatizada, el sistema informático utilizado. Es importante resaltar que la existencia del registro de incidencias es obligatoria en todos los casos y no está supeditada a que se haya producido una en el pasado.

2.3 Control de acceso

Se encuentra regulada en el artículo 91 del Reglamento de desarrollo de la LOPD:

«1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio».

Por tanto, la norma establece que los usuarios autorizados para el acceso a datos de carácter personal, sólo deben poder acceder a los datos que **sean relevantes y necesarios**, para el desempeño de sus funciones. Corresponde al responsable del fichero implantar un sistema de

permisos de acceso tanto si es fichero es automatizado como si es no automatizado. También en necesario tener en cuenta la previsión contenida en el apartado cuarto que obliga a los responsables del fichero a determinar quiénes serán las personas autorizadas para conceder, alterar o anular los accesos autorizados.

2.4 Gestión de soportes y documentos

Se encuentra regulada en el artículo 92 del Reglamento de Desarrollo de la LOPD:

«1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas».

Por tanto, los soportes -cartuchos, cintas, disquetes, discos, etc.- que contengan datos personales deben identificar el tipo de información que contienen. En este sentido debe tenerse en cuenta la definición de soporte contenida en el Reglamento de desarrollo de la LOPD, y que considera soporte todo aquel objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos. No obstante también debe tenerse en cuenta que el Reglamento de desarrollo de la LOPD también impone obligaciones en relación con el tratamiento de **documentos** que incluyan datos personales[193].

Por tanto, deberemos tener en cuenta que se deberán implantar medidas de seguridad adicionales en relación a la salida de los soportes o documentos, a su destrucción y a su etiquetado:

- **Salida de soportes:** Deberá ser siempre autorizada por el responsable del fichero o encontrarse autorizada en el documento de seguridad. Además se deberá tener en cuenta que dentro de esta salida de soportes o documentos se podrá realizar incluso mediante correo electrónico o a través de dispositivos portátiles siendo necesario adoptar las medidas que se estimen necesarias para evitar la sustracción, pérdida o acceso indebido a la información objeto de traslado.
- **Desechado de soportes:** Se deberán adoptar medidas tendentes a evitar el acceso o recuperación de los datos personales contenidos en soportes o documentos, en caso de que proceda a su desechado.
- **Etiquetado de soportes:** Se deberá tener en cuenta que:
  - El etiquetado deberá permitir identificar el tipo de información que contiene el soporte.
  - En caso de soportes que contengan datos personales especialmente sensibles, el etiquetado podrá ser comprensibles y con significado solo para usuarios autorizados de forma que se dificulte la identificación para el resto de personas.

2.5 Identificación y autenticación

Esta medida de seguridad se encuentra regulada en el artículo 93 del Reglamento de Desarrollo de la LOPD:

193 El concepto de documento se encuentra definido en el Reglamento de desarrollo de la LOPD como «*todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que pueda ser tratada en un sistema de información como unidad diferenciada*».

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Tal y como establece el artículo 5 del Reglamento de desarrollo de la LOPD, se entiende por identificación y autenticación:

- **Identificación:** procedimiento de reconocimiento de la identidad de un usuario.
- **Autenticación:** procedimiento de comprobación de la identidad de un usuario.

Ya hemos tenido oportunidad de ver que el Reglamento de desarrollo de la LOPD exige que exista una "*relación actualizada de usuarios y accesos autorizados*". En relación con esta obligación, y a la vista de lo establecido por el artículo 93, hemos de entender que aquellos responsables de ficheros que gestionen datos de carácter personal, deberán contar con un **procedimiento de gestión de usuarios**, que garantice la correcta identificación y autenticación del usuario. Es decir, deberán establecerse las garantías suficientes para determinar que la persona que accede a los datos es quien dice ser, que se ha comprobado su identidad, que dispone de mecanismos de acceso al sistema que evitan su suplantación y que en cada acceso se verifica que el usuario está autorizado.

En relación a la gestión de contraseñas, el Reglamento de desarrollo de la LOPD exige que:

- Se deberá disponer de un procedimiento que garantice la confidencialidad de las

contraseñas, lo que incluye la obligación de garantizar que la asignación, distribución y almacenamiento se realice en condiciones de confidencialidad.

- La duración de la validez de estas las contraseñas, no puede superar el límite máximo de **un año**.

Asimismo es conveniente que el procedimiento establecido tenga en cuenta otros aspectos respecto a la gestión de las contraseñas:

- Si la contraseña es generada de forma automática es conveniente que el sistema obligue al usuario a su modificación en el primer acceso.
- Determinar una longitud de las contraseñas que las haga seguras y poco vulnerables a ataques de fuerza, siendo altamente recomendable que el procedimiento exija la inclusión de letras, números y caracteres especiales en las contraseñas.
- Establecer límites de frecuencia en la utilización de contraseñas; esto es decir, impedir que el usuario pueda repetir las últimas contraseñas utilizadas.
- Establecer sistemas de bloqueo y desbloqueo de contraseñas que entrarán en funcionamiento en reintentos de acceso fallidos u otros casos en los que el usuario entienda que la confidencialidad de su clave ha podido ser comprometida.

2.6 Copias de respaldo y recuperación

Se encuentran reguladas en el artículo 94 del Reglamento de Desarrollo de la LOPD:

«1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
*4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una c*opia de seguridad».

Las copias de respaldo o *backups* tienen como finalidad garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento anterior a que se produjera la pérdida o destrucción de la información. En esencia este tipo de procedimientos se diseñan para garantizar:

- La reconstrucción del sistema operativo y su configuración.
- La reinstalación y puesta en funcionamiento del software base y de las aplicaciones necesarias para el tratamiento de los datos.
- Los archivos, documentos y bases de datos objeto de tratamiento.

Cuando los sistemas de información gestionen datos personales, la realización de estos procedimientos de respaldo resulta obligatoria. En concreto, para que estos procedimientos se ajusten a lo previsto por el Reglamento de desarrollo de la LOPD deberá establecerse un procedimiento de copias de *back-up* mediante el cual el responsable del fichero debe garantizar que:

- La copia de seguridad se realiza **al menos semanalmente**, salvo que no existan cambios.
- El procedimiento incluye la realización de una revisión del buen funcionamiento de los sistemas de *back-up* con una frecuencia **mínima de seis meses.**

Asimismo, el Reglamento de desarrollo de la LOPD prevé la posibilidad de que existan **tratamientos mixtos** estableciéndose unas pautas con el objetivo de garantizar que la introducción manual de la información afecte lo menos posible a la integridad de los datos. Para poder llevar a

cabo una recuperación parcialmente manual deberán darse las siguientes condiciones:

- Que la destrucción afecte a ficheros o tratamientos parcialmente automatizados.
- Que exista documentación que permita la reconstrucción de los datos al estado en que se encontraban en el momento previo a la incidencia.
- Que quede constancia motivada de este hecho en el Documento de Seguridad.

Para finalizar, conviene recordar que el Reglamento de Desarrollo de la LOPD también regula el desarrollo de pruebas sobre entornos que traten datos de carácter personal ya que es evidente que dichas prácticas pueden afectar a la confidencialidad e integridad de los datos personales y por ello cuando se realicen pruebas de este tipo:

- Se tenderá a evitar el uso de datos reales para estas tareas.
- En caso de que se deseen utilizar datos reales, se deberá garantizar el nivel de seguridad correspondiente al tratamiento realizado.
- Las pruebas deberán quedar reflejadas en el Documento de Seguridad.
- De forma previa se habrá realizado una copia de seguridad de los datos personales utilizados.

3. Medidas de seguridad de nivel medio en los ficheros automatizados

3.1 Responsable de Seguridad

La presente medida se encuentra regulada en el artículo 95 del Reglamento de Desarrollo de la LOPD:

«En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento».

La figura detallada en el artículo 95 del Reglamento deberá quedar plasmada y fijada en el Documento de Seguridad cuando el responsable del fichero lleve a cabo tratamientos de datos personales sobre los cuales se deban aplicar las medidas de seguridad de nivel medio. En este sentido el Responsable de Seguridad es la persona encargada de velar por el cumplimiento de las medidas, reglas y normas de seguridad establecidas por el Responsable del fichero. No obstante, tal y como establece el Reglamento de Desarrollo es posible designar varios responsables de seguridad que trabajarán de forma coordinada en otros ámbitos de la organización como el jurídico o el informático, entre otros.

El artículo 95 del Reglamento de desarrollo de la LOPD tiene como predecesor el artículo 16 del Reglamento de Medidas de Seguridad, que establecía:

«El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad.
En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento».

Como se puede observar las diferencias son mínimas entre ambos artículos. Por tanto, la figura del Responsable de Seguridad se mantiene prácticamente en los mismos términos, y es posible, basarse el Informe de la Agencia Española de Protección de Datos, del año 1999, que interpretó el contenido del artículo 16 del Reglamento de Medidas de Seguridad y determinó las funciones de la figura del Responsable de Seguridad:

«El artículo 16 del Reglamento, señala que "el responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento".

El Reglamento no especifica de forma taxativa los requisitos que habrá de cumplir este responsable de seguridad, si bien los mismos se desprenden de sus propias funciones, ya que le corresponderá, como se ha indicado "coordinar y controlar las medidas definidas en el documento de seguridad", analizando el contenido del informe de auditoría con el fin de proponer la adopción de las medidas

pertinentes.

Por ello, sin perjuicio de que su configuración habrá de depender según el tamaño de la empresa o la existencia de uno o varios centros de actividad, habrá de ser una persona con los conocimientos suficientes para llevar a cabo eficazmente estas funciones, adoptando las medidas necesarias para el cumplimiento de las medidas exigibles.

Además, debe añadirse que la delimitación del concepto de responsable de seguridad no exige que el mismo sea distinto del propio responsable del fichero, dependiendo esta circunstancia de la actividad llevada a cabo por éste.
Por otra parte, debe indicarse que el responsable del seguridad no aparece como responsable a efectos de la imposición del régimen sancionador previsto en la LOPD, recayendo tal responsabilidad sobre el responsable del fichero y el encargado del tratamiento».

En base al contenido del artículo 95 del Reglamento de desarrollo de la LOPD así como en base a la interpretación de la Agencia Española de Protección de Datos, es posible determinar de forma concreta, cuales son las funciones del Responsable de Seguridad y que habrán de ser incluidas en el Documento de Seguridad.

Básicamente nos encontramos en presencia de funciones de coordinación y control de aplicación de las medidas de seguridad constituyendo la presente lista, una lista abierta que sirva como orientación y guía sin que por ello quiera decir que son las únicas que puedan atribuirse a la presente figura:

- Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.
- Determinar y describir los recursos de información que se encontrarán sujetos al Documento de Seguridad. Corresponde al Responsable garantizar que no existen en la organización tratamientos de datos de carácter personal sin identificar, que puedan suponer un riesgo para el Responsable del fichero.
- Controlar y coordinar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
- Controlar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos así como su periodicidad.
- Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado a los

recursos de información, con especificación del nivel de acceso que tiene cada usuario.

- Controlar y coordinar la aplicación del procedimiento de identificación y autenticación de usuarios, lo que incluye el control de la asignación, distribución y almacenamiento de las contraseñas de acceso.
- Controlar la aplicación de las normas internas para el cambio periódico de las claves de acceso y contraseñas de los usuarios del sistema.
- Comprobar la existencia y aplicación de un sistema que limite el acceso de los usuarios exclusivamente a aquellos datos y recursos que en cada caso precisen para el desarrollo de sus funciones.
- Establecer y comprobar la aplicación de los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados. Cuando el responsable del tratamiento deba aplicar las medidas de seguridad de nivel alto será necesario, tal y como podremos ver más adelante, que se implante una medida de seguridad denominada Registro de accesos. Dicho Registro estará bajo el control directo del Responsable de Seguridad, que deberá velar por su mantenimiento, garantizando a un tiempo que el sistema utilizado no permita en ningún caso su desactivación. En estos supuestos, el Responsable de Seguridad revisará periódicamente la información de control registrada y elaborará un informe periódico en el que se incluirán las incidencias en el acceso a los datos personales responsabilidad de la organización.
- En su caso, conceder, modificar y anular el acceso autorizado a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.
- Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas y estableciendo controles periódicos y las auditorias necesarias para comprobar el nivel de cumplimiento del Documento de Seguridad.

3.2 Auditoría

Se encuentra regulada en el artículo 96 del Reglamento de Desarrollo de la LOPD:

«1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen

modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas».

Corresponde al responsable del fichero auditar el cumplimiento de las obligaciones recogidas en el Título VIII Reglamento de desarrollo de la LOPD para todos los sistemas que incluyan tratamientos de datos personales clasificados como de nivel medio y alto, auditoría que se llevará a cabo al menos de forma bienal admitiéndose auditorías de carácter interno y de carácter externo.

En el año 1999 la Agencia Española de Protección de Datos emitió un Informe analizando la obligación recogida en el ya derogado artículo 17 del Reglamento de Medidas de Seguridad, que el artículo 96 Reglamento de desarrollo de la LOPD ha venido a sustituir:

«***Alcance de la auditoría a que se refiere el Reglamento.***
El artículo 17 dispone, junto con la obligación general de someter los sistemas e instalaciones a auditoría y el contenido de ésta que "los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos". De ello se desprende que, una vez elaborado el informe de auditoría, deberán comunicarse sus resultados, adoptándose las medidas pertinentes, sin que ello exija una "aprobación" formal y externa de su contenido, que no habrá de ser remitido a la Agencia Española de Protección de Datos, sino "puesto a su disposición". Ello supone que será el responsable del tratamiento, siguiendo las recomendaciones del responsable de seguridad quien habrá de implantar las medidas precisas, derivadas del informe, de forma que, en caso de no

implantarse y no cumplirse los requisitos de seguridad establecidos en el Reglamento, incurrirá en responsabilidad, constitutiva de infracción grave según el artículo 44.3 h) de la LOPD, lo que se comprobará por esta Agencia Española de Protección de Datos a través del examen, en su caso, del informe de auditoría y de la implantación efectiva de las medidas requeridas. Asimismo, se ha planteado en varias ocasiones si el sistema de auditoría establecido en la norma cuarta de la Instrucción 1/1995, de la Agencia Española de Protección de Datos, de 1 de marzo, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito y del artículo 17 del Reglamento de Medidas de Seguridad se refieren a un mismo supuesto.

La respuesta a esta cuestión es afirmativa, dado que el contenido de ambas auditorias es similar, de forma que el artículo 17.2 del Reglamento de Medidas de Seguridad no hace sino reiterar, para la totalidad de los ficheros sometidos al nivel medio de seguridad, en los términos establecidos en el artículo 4.2 del propio Reglamento, lo que ya disponía el apartado quinto de la norma cuarta de la Instrucción 1/1995, diferenciándose únicamente ambos supuestos en que el Reglamento de Medidas de Seguridad no exige la remisión del informe de auditoria a la Agencia, quedando éste sin embargo a disposición de la misma.

En consecuencia, teniendo en cuenta que el Reglamento de Medidas de Seguridad es norma posterior reguladora de la misma materia que la Instrucción 1/1995, en cuanto a los ficheros a los que se refiere el artículo 29 de la LOPD, habrá de entenderse que la norma cuarta de la Instrucción ha sido derogada por el artículo 17 del Reglamento, siendo este el que habrá de regir en lo sucesivo para todos los ficheros sujetos a medidas de seguridad de nivel medio, entre los que se encuentran los relacionados con la solvencia patrimonial y crédito de las personas físicas».

El presente artículo pretende otorgar a los Responsables de Fichero de una herramienta para identificar posibles incumplimientos, permitiéndole así establecer las bases para su subsanación: El Informe de Auditoría deberá dictaminar sobre el grado de adecuación y cumplimiento de las medidas de seguridad, identificar sus deficiencias y proponer las medidas correctoras necesarias.

La principal novedad con respecto a la normativa anterior se encuentra en que la obligación de realizar auditorías no se limitará al periodo señalado de dos años como máximo, sino que se establece también la obligación de auditar los sistemas de información siempre que se hayan producido *modificaciones sustanciales* en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

3.3 Gestión de soportes y documentos

La presente medida se encuentra regulada en el artículo 97 del Reglamento de Desarrollo de la LOPD:

«1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada».

Estas medidas adicionales -para los ficheros de nivel medio y alto- y que en el Reglamento de Medidas de Seguridad se extendían también a las obligaciones relativas al control de la salida de estos soportes y documentos y a su destrucción, han quedado limitadas a la existencia de un registro de entrada y salida, ya que, como hemos visto, el Reglamento de desarrollo de la LOPD ha extendido las demás a todos los ficheros de datos personales en virtud de su artículo.

La presente medida supone la implantación de procedimientos y normas de gestión que permitan establecer un canal de autorizaciones para la entrada y salida de soportes informáticos y documentos que contengan datos de carácter personal a los que sea aplicable el nivel medio de seguridad. Dichos Registros así como el procedimiento de gestión y autorización de entrada y/o salida deberán quedar definidos en el Documento de Seguridad.

3.4 Identificación y autenticación

La presente medida de seguridad se encuentra regulada en el artículo 98 del Reglamento de desarrollo de la LOPD:

«El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información».

A través del presente artículo se establecen medidas adicionales a lo ya establecido para los ficheros de nivel básico como la obligación de establecer un mecanismo para evitar los reintentos de acceso a los ficheros que contengan datos sobre los que se deba aplicar las medidas de seguridad de nivel medio o alto.

Por tanto el cumplimiento de esta medida de seguridad implica el establecimiento de un mecanismo de bloqueo que deberá operar tanto para accesos en modo local como en red, y que permitirá al responsable de seguridad evitar vulnerabilidades, estableciendo controles de seguridad para que usuarios no autorizados no puedan utilizar contraseñas de acceso de terceros.

3.5 Control de acceso físico

Se encuentra regulada en el artículo 99 del Reglamento de Desarrollo de la LOPD:

«Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información».

La presente medida de seguridad es de aplicación exclusiva a los ficheros automatizados de nivel medio y alto debiendo tenerse en cuenta que no ha sufrido modificación respecto a lo establecido por el Reglamento de Medidas de Seguridad. Por tanto, únicamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales en donde se encuentren ubicados los sistemas de información con datos de carácter personal. Este control de acceso físico deberá ser aplicado en todos aquellos lugares en los que se hallen instalados equipos que den soporte a los sistemas de información que gestionen datos personales. Por tanto, la medida afectará tanto a los Centros de Procesamiento de Datos como a aquellas salas en las que se ubiquen los Servidores que contengan datos de carácter personal.

En cuanto a las medidas de seguridad concretas, el Reglamento no aporta concreción alguna sobre cuáles pueden ser por lo que el responsable del fichero se verá obligado a utilizar la lógica y el sentido común. No obstante pueden servir de guía las siguientes medidas:

- Acceso restringido exclusivamente al personal autorizado. Este acceso podrá realizarse mediante el uso de claves, llaves físicas, tarjetas electrónicas o cualquier otro dispositivo

que garantice el acceso de las personas a las que les ha sido autorizado el acceso.

- Pueden establecerse medidas adicionales, como el establecimiento de sistemas de registro que permitan la identificación de los accesos realizados por personal autorizado.
- Aquellos lugares en los que se instalen los equipos físicos que contengan datos personales deberán reunir las condiciones que permitan garantizar la seguridad de los datos siendo recomendable la implantación de medidas adicionales como pueden ser el uso de sistemas redundantes de alimentación, sistemas de refrigeración así como sistemas contra incendios.

3.6 Registro de incidencias

Se encuentra regulada en el artículo 100 del Reglamento de Desarrollo de la LOPD:

«1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos».

La importancia de los datos sobre los que se aplican las medidas de seguridad medio obligan a que el control ya establecido, para las medidas de seguridad de nivel medio, incluya más información que permita, por un lado, garantizar que las incidencias son gestionadas por personal autorizado por el responsable del fichero, y por otro, que se establece un registro adecuado de los datos restaurados que permitirán establecer una trazabilidad de las acciones realizadas.

Cuando nos encontremos en presencia de datos personales sobre los que se deban aplicar las medidas de seguridad de nivel medio, el registro de incidencias deberá contener además de los datos ya consignados, los siguientes:

- Procedimientos realizados de recuperación de los datos.
- Persona que ejecutó el proceso.
- Responsable que autorizó el proceso.
- Datos restaurados.
- En su caso, datos que se han restaurado manualmente.

4. Medidas de seguridad de nivel alto en los ficheros automatizados

4.1 Gestión y distribución de soportes

La presente medida de seguridad se encuentra regulada en el artículo 101 del Reglamento de Desarrollo de la LOPD:

«1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos».

Cuando nos encontramos en presencia de datos personales sobre los que se deba aplicar el nivel de seguridad alto, el Reglamento habla exclusivamente de soportes, y no de soportes y documentos, tal y como sucedía cuando hacíamos referencia a las medidas de seguridad de nivel básico.

En este sentido, destaca la obligación establecida por el Reglamento de desarrollo de la LOPD de establecer un sistema de etiquetado confidencial. Hablamos por tanto, de una obligación y no de una opción para el Responsable del fichero exigiéndose, además, que la identificación de los soportes tenga las siguientes características:

- Que sea comprensible para los usuarios con acceso autorizado, que podrán identificar de esta forma su contenido.
- Que dificulte su identificación para terceros no autorizados

Asimismo, el presente artículo o medida de seguridad establece una serie de normas para la distribución de los soportes. Cuando los mismos salgan de sus locales, el Responsable del fichero estará obligado a realizar la distribución cifrando los datos o utilizando un procedimiento alternativo recogiéndose, expresamente, esta obligación para los dispositivos portátiles. Por tanto, podemos observar que el Reglamento responde así a la utilización de este tipo de dispositivos cada vez más extendidos.

4.2 Copias de respaldo y recuperación

La presente medida se recoge en el artículo 102 del Reglamento de Desarrollo de la LOPD:

«Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación».

La presente medida de seguridad establece la obligación de conservar una copia de respaldo en un lugar distinto de los locales en los que se encuentran instalados los equipos que los tratan. La copia debe incluir no solo los datos personales, sino también los procedimientos de recuperación.

En este punto debe tenerse en cuenta la obligatoriedad de que el lugar escogido para el almacenamiento de estas copias de respaldo deberá cumplir con todas las exigencias de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la LOPD.

Una de las novedades del Reglamento de Desarrollo de la LOPD sobre su predecesor, el Reglamento de Medidas de Seguridad, es que el primero permite que puedan utilizarse procedimientos alternativos al envío de copias fuera de los locales (sistemas de *back-up* alternativos, situados en un lugar diferente), y que en todo caso garanticen la integridad y la recuperación de la información.

4.3 Registro de accesos

La presente medida de seguridad se encuentra establecida en el artículo 103 del Reglamento de desarrollo de la LOPD:

«1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

5. *El período mínimo de conservación de los datos registrados será de dos años.*
6.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

- Que el responsable del fichero o del tratamiento sea una persona física.

- Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad».

La presente medida de seguridad es una de las más gravosas para los Responsables de ficheros que

tratan datos de carácter personal y sobre la cual la Agencia Española de Protección de Datos ya tuvo oportunidad de pronunciarse en uno de sus informes en el año 1999:

«También resulta ser objeto de consulta el sentido en que se debe interpretar la medida relacionada con el registro de accesos, a la que se refiere el artículo 24 del Reglamento de Medidas de Seguridad, por cuanto se consideraba que la indicación de la totalidad de los extremos indicados en la norma podía resultar sumamente gravosa para la responsable del fichero.

Para realizar una correcta interpretación de la exigencia impuesta por esta norma, debe partirse de la regulación establecida con carácter general en el Reglamento para regular las medidas que garanticen un adecuado acceso a los ficheros que contengan datos de carácter personal. Dichas medidas se circunscriben a las previsiones contenidas en los artículos 12 y 19 del Reglamento, en lo referente al establecimiento de controles de acceso y acceso físico para los ficheros sujetos a medidas de nivel bajo y medio, respectivamente, y el ya citado artículo 24.

El artículo 2.7 del Reglamento define el control de acceso como el "mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos". En estos términos el artículo 12 se refiere al acceso como cualquier actuación por la que un usuario pueda tener conocimiento directo de "aquellos datos y recursos que precisan para el desarrollo de sus funciones". En desarrollo de este concepto, para los ficheros a los que el Reglamento quiere dotar de un máximo nivel de seguridad, el artículo 24 exige la llevanza del registro de acceso al que ya se ha hecho referencia.

De todo ello se desprende que el Reglamento no establece diferenciación alguna en atención a la persona que accede a los datos o de las actividades que aquella lleva a cabo, por lo que en el registro deberán figurar la totalidad de los accesos que se hayan producido».

Como podemos observar, la propia Agencia Española de Protección de Datos reconoce la carga que se impone, justificándolo en el *máximo nivel de seguridad* del que se quiere dotar a los datos personales sobre los que se deben aplicar las medidas de seguridad nivel alto.

Si bien la entrada en vigor del Reglamento de desarrollo de la LOPD ha supuesto un incremento de estas obligaciones en términos generales, el Reglamento ha tenido en cuenta la posible desproporción de su aplicación en algunos casos y ha reconocido una serie de excepciones de las que hablaremos más adelante.

En relación a este tipo de registros hemos de decir que deberán conservar la siguiente información por cada intento de acceso a los datos:

- Identificación del usuario
- Fecha y hora en la que se realizó el intento de acceso
- Fichero accedido
- Tipo de acceso
- Resultado del intento de acceso: autorizado/denegado
- Cuando el acceso haya sido autorizado, se registrará también el registro accedido. En todo caso se deberá conservar la información necesaria para identificar el registro accedido y el hecho de su modificación sin que, a juicio de la Agencia Española de Protección de Datos, la obligación alcance a la conservación del contenido concreto del mismo.

En relación a las excepciones que citábamos con anterioridad, el Reglamento de Desarrollo establece que no será necesario este registro de accesos siempre y cuando se produzcan alguna de estas circunstancias:

- Que el Responsable del Fichero o del tratamiento sea una persona física.
- Que el Responsable del Fichero o del tratamiento garantice que únicamente él tiene acceso a los datos personales.

Otras obligaciones que es necesario considerar en la implantación de esta medida de seguridad son:

- Mecanismos que permitan el registro estarán bajo el control directo del Responsable de Seguridad competente sin que este deba permitir su desactivación o manipulación.
- Que el periodo mínimo de conservación de estos datos será como mínimo de dos años. El Reglamento no indica nada respecto a la forma de conservación de esta información por lo que debe entenderse que será suficiente con que se establezcan los mecanismos que garanticen la recuperación de la información durante el periodo establecido.
- El Responsable de Seguridad se encargará de revisar al menos una vez al mes la información registrada y elaborará un informe de las revisiones realizadas y de los problemas detectados.

4.4 Telecomunicaciones

La presente medidas de seguridad se encuentra regulada en el artículo 104 del Reglamento de Desarrollo de la LOPD:

«Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros».

El principal punto de aplicación de esta medida es la transmisión de datos a través de Internet y para su análisis es necesario apoyarse en un informe realizado por la Agencia Española de Protección de Datos en 1999 y que responde a una consulta en relación al ámbito de aplicación de la obligación y de la posibilidad de que la misma resulte aplicable a las comunicaciones realizadas entre distintos locales de un mismo Responsable del tratamiento:

«El artículo 26 del Reglamento de Seguridad exige el cifrado de datos cuando los mismos van a ser transmitidos a través de redes de telecomunicaciones.

En cuanto al ámbito de aplicación del artículo 26, aplicable únicamente a los ficheros que requieran medidas de seguridad de nivel alto, debe estarse al hecho de que en la transmisión de los datos se empleen redes de telecomunicaciones, definidas por el artículo 2. c) de la Directiva 97/66/CE, de 15 de diciembre, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, como "los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por otros medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicaciones".

En consecuencia, las medidas a las que se refiere el artículo 26 del Reglamento serán de aplicación a la transmisión de datos entre distintas dependencias de la entidad cuando sea necesaria para dicha transmisión la utilización de redes de telecomunicaciones cuya titularidad sea ajena a la propia empresa, no siendo preciso el cifrado de los datos en caso de que las comunicaciones en ningún momento accedan a dicha red».

Como podemos observar las únicas variaciones en relación a lo estipulado por el derogado Reglamento de Medidas de Seguridad son las siguientes:

- La referencia expresa a los datos que, conforme al artículo 81.3 Reglamento de desarrollo de la LOPD, tendrán la consideración de datos de nivel alto.
- La referencia a las *redes públicas o redes inalámbricas de comunicaciones electrónicas.*

5. Medidas de seguridad en los ficheros automatizados

Hasta la entrada en vigor del Reglamento de Medidas de Seguridad, los ficheros no automatizados de datos personales debían aplicar medidas de seguridad de acuerdo a lo establecido en la LOPD. Sin embargo, el artículo 1 del Reglamento de Medidas de Seguridad delimitaba su ámbito de aplicación estableciendo que la norma era aplicable únicamente a los ficheros automatizados ya que no debemos olvidar que dicho Reglamento se ajustaba a lo establecido por la LORTAD. Con la entrada en vigor de la LOPD, se amplió el ámbito de aplicación de esta materia, alcanzando a los datos de carácter personal registrados en soporte físico que los hace susceptibles de tratamiento y a toda modalidad de uso posterior de los mismos por lo que evidentemente los tratamientos en soporte papel caían dentro del ámbito de aplicación de la LOPD.

En este escenario, la Disposición Transitoria Tercera de la LOPD mantuvo la vigencia de las normas reglamentarias preexistentes, entre las que expresamente se citaba el Reglamento de Medidas de Seguridad, en cuanto no se oponía a la nueva Ley, a la espera de un nuevo desarrollo reglamentario. A través de esta fórmula, desde la entrada en vigor de la LOPD, resultó aplicable el Reglamento de Medidas de Seguridad a los ficheros en soporte no automatizado que se hubieran creado con posterioridad al 14 de enero del año 2000**.** En cuanto a los ficheros en soportes no automatizados que existieran antes de dicha fecha, se dispuso un plazo para su adaptación establecido en la Disposición Adicional Primera y que finalizó en octubre de 2007.

No obstante, muchos de los aspectos contenidos en el Reglamento de Medidas de Seguridad no eran susceptibles de aplicarse, conforme a los criterios expuestos, a los ficheros no automatizados. Por ello, durante todo el periodo de vigencia de la LOPD, sólo debieron implantarse las medidas de seguridad que, pese a estar previstas para tratamientos automatizados, por su naturaleza también resultaban aplicables a ficheros no automatizados como, por ejemplo, la elaboración e implantación

del Documento de Seguridad. Este régimen cambió de forma radical con la entrada en vigor del Reglamento de desarrollo de la LOPD que en su Disposición Derogatoria Única, establece:

«Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente Real Decreto».

Una de las novedades que mayor expectación han levantado el Reglamento de desarrollo es la relativa a las medidas de seguridad que serán de aplicación a los ficheros contenidos en soporte papel. Debemos comenzar su análisis destacando que, al igual que para los ficheros automatizados, en el caso de los ficheros no automatizados se mantienen los tres niveles de seguridad: básico, medio y alto. Por lo demás, el Reglamento de desarrollo de la LOPD regula toda una serie de medidas de seguridad, específicas para los ficheros no automatizados y que se encuentran recogidas en el Capítulo IV de su Título VIII

5.1 Medidas de seguridad: Niveles Básico y Medio

5.1.1 Obligaciones comunes

A la hora de analizar las medidas de seguridad previstas para los ficheros no automatizados, no podemos pasar por alto que muchas de las medidas previstas para los ficheros automatizados son de obligado cumplimiento también para los ficheros no automatizados. Hablamos de medidas generales cuya aplicación no depende del soporte y que por tanto, deben ser aplicadas para cualquier tipo de fichero o tratamiento de datos de carácter personal. En este sentido el artículo 105 recoge cuales son las citadas obligaciones comunes:

«1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a. Alcance.
b. Niveles de seguridad.

c. Encargado del tratamiento.

d. Prestaciones de servicios sin acceso a datos personales.

e. Delegación de autorizaciones.

f. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

g. Copias de trabajo de documentos.

h. Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a. Funciones y obligaciones del personal.

b. Registro de incidencias.

c. Control de acceso.

d. Gestión de soportes».

5.1.2 Criterios de archivo

Se encuentra regulada en el artículo 106 del Reglamento de Desarrollo de la LOPD:

«El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo».

En primer lugar, se establece la obligación de respetar los criterios que, en su caso, pueda establecer la legislación aplicable a la documentación. En caso contrario, queda bajo la responsabilidad del responsable del fichero el establecer los criterios y procedimientos de actuación que deberán seguirse para el archivo de la documentación que contenga datos personales. En este sentido resulta recomendable elaborar una política específica que establezca las directrices para el tratamiento de esta documentación. Dichas directrices, a su vez, deberán estar respaldadas por los procedimientos de actuación correspondientes.

Para la elaboración de estas políticas, el legislador solo establece los siguientes requisitos:

- Los criterios utilizados deberán garantizar la conservación en condiciones de seguridad. Deberán tenerse en cuenta, tanto las condiciones de acceso y seguridad de los dispositivos de archivo, como las condiciones ambientales y los riesgos a los que la documentación pueda quedar expuesta.
- Deberán garantizar también la localización y consulta de la información. El Reglamento de desarrollo de la LOPD exige por lo tanto que se garantice la disponibilidad de la información sin entrar a especificar los criterios mediante los que se podrá alcanzar este objetivo, quedando los mismos a iniciativa del responsable del fichero.
- Los criterios utilizados deberán permitir el correcto ejercicio de los derechos de acceso, rectificación, cancelación y oposición por parte de los titulares de los datos.

5.1.3 Dispositivos de almacenamiento

La presente medida de seguridad se encuentra recogida en el artículo 107 del Reglamento de Desarrollo de la LOPD:

«Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.
Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas».

Debemos observar que la presente medida de seguridad es demasiado genérica, limitándose a la exigencia de contar con dispositivos de almacenamiento -armarios, archivadores, cajones, etc.-, que cuenten con un dispositivo que permita controlar su apertura como llaves o candados.

De forma adicional se permite la adopción de medidas alternativas en los casos en los que las características físicas de las instalaciones del responsable del fichero no permitan la implantación de estas medidas. No obstante tampoco se indica ningún criterio, por lo que podrán plantearse distintas medidas que, combinadas, permitan garantizar un nivel de seguridad equivalente al que se alcanzaría mediante el uso de estos mecanismos de cierre de los dispositivos de almacenamiento como pueden ser:

- Colocación de carteles prohibiendo el acceso.
- La custodia de los documentos por personal humano.

5.1.4 Custodia de soportes

Se encuentra regulada en el artículo 108 del Reglamento de Desarrollo de la LOPD:

«Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada»

La presente medida regula la situación en la que la documentación no se encuentre archivada y por tanto resulte accesible a cualquier persona con acceso a las instalaciones del responsable del fichero. En este caso tampoco se detallan obligaciones concretas, más allá de establecer la responsabilidad de la persona que esté tramitando el documento, que tendrá una obligación genérica de custodia. En este sentido es recomendable que el responsable del fichero adopte normas internas en relación al tratamiento de la documentación.

5.1.5 Responsable de seguridad y auditorías

Los artículos 109 y 110 Reglamento de desarrollo de la LOPD se refieren a la necesidad de nombrar uno o varios responsables de seguridad así como a la obligación de realizar auditorías de cumplimiento cuando se estén llevando a cabo tratamientos no automatizados de nivel medio. El contenido de estos artículos es el siguiente y que como podemos observar no difieren de lo ya analizado en el caso de los ficheros o tratamientos automatizados:

***«Artículo 109. Responsable de seguridad**.*
Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título».

5.2 Medidas de seguridad: Nivel Alto

5.2.1 Almacenamiento de la información

La presente medida se encuentra regulada en el artículo 108 del Reglamento de Desarrollo de la LOPD:

«1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad».

Nos encontramos en presencia de una medida cuyo cumplimiento, en principio, no debe ofrecer problema al Responsable del Fichero. De hecho, la mayoría de las organizaciones habrán dispuesto ya estas áreas de acceso protegido para la custodia de la información que consideran sensible o estratégica. Por otro lado, en caso de que no sea posible la implantación de estas medidas de seguridad -en razón de las características de las instalaciones y de los recursos disponibles- se prevé la posibilidad de adoptar medidas alternativas.

5.2.2 Copia o reproducción

La presente medida de seguridad se encuentra regulada en el artículo 112 del Reglamento de Desarrollo de la LOPD:

«1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior».

La presente medida de seguridad no exige que se realicen copias de respaldo o seguridad. Únicamente hace referencia a la necesidad de que las copias que se realicen sean realizadas bajo la supervisión del personal autorizado, personal que constará en el Documento de Seguridad. En lo relativo a la destrucción de las copias, se establece también otra medida de cara a evitar el acceso no autorizado a los datos por parte de terceros. En este supuesto, resulta conveniente establecer medios para que el personal proceda a la destrucción de las copias, tales como destructoras de papel, contenedores específicos para la destrucción de documentos o la contratación de empresas especializadas en la destrucción segura de documentación.

5.2.3 Acceso a la documentación

La presente medida de seguridad se recoge en el artículo 113 del Reglamento de Desarrollo de la LOPD:

«1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad».

Por tanto, solamente el personal autorizado podrá acceder a la documentación que contenga datos

personales sobre los que se deban aplicar las medidas de seguridad de nivel alto. Personal que, por otra parte, deberá quedar identificado en el Documento de Seguridad, bien de forma nominativa, bien a través de su cargo o perfil de actividad.

En relación al establecimiento de mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios, nos encontramos en presencia de una medida que pretende equiparar los ficheros no automatizados con el control exigido a los ficheros automatizados a través del registro de accesos. En este sentido se deben tener en cuenta las siguientes consideraciones:

- Cuando un documento solamente pueda ser utilizado por un usuario, no será necesario identificar los accesos realizados.
- En caso de documentos que deban ser utilizados por múltiples usuarios, deberá establecerse en el Documento de Seguridad un mecanismo para que quede registrado cada uno de los accesos. Estos mecanismos habitualmente se basarán en la utilización de plantillas básicas en soporte papel que se incorporarán al comienzo del expediente y en las que se irán haciendo constar los accesos.

5.2.4 Traslado de la documentación

El traslado de la documentación se encuentra regulado en el artículo 114 del Reglamento de Desarrollo de la LOPD:

«Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado».

Como podemos observar se trata de una medida de seguridad excesivamente genérica y que obliga al responsable del fichero a realizar un auténtico esfuerzo de imaginación. En todo caso, las siguientes pueden ser algunas de las medidas, enumeradas a modo meramente ejemplificativo:

- Contratación de servicios de externos.
- Elaboración de protocolos para detectar la apertura o manipulación de la documentación enviada: firmas, sellos, lacres, de forma que se puedan obtener indicios de que se ha producido un acceso o manipulación.

IV. AUDITORÍAS

1. Régimen jurídico

La obligación de auditar tiene su origen en el principio de seguridad enunciado por el artículo 9 de la LOPD. En dicho texto, cuyo contenido es prácticamente idéntico, al que enunciaba la LORTAD, establece la obligación de adoptar medidas de seguridad para el responsable del fichero y para el encargado de tratamiento:

«El responsable del fichero, y, en su caso, el encargado del tratamiento deberán 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 estén expuestos, ya provengan de la acción humana o del medio físico o natural».

Como podemos observar el artículo 9 de la LOPD persigue garantizar los siguientes objetivos de seguridad:

- ***Integridad:*** En el sentido de mantener la exactitud de la información que debe también ser completa, así como sus métodos de proceso.
- ***Disponibilidad:*** O lo que es lo mismo, el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.
- ***Confidencialidad:*** El acceso a la información únicamente por quienes estén autorizados.

Como ya hemos tenido oportunidad de ver el artículo 96 del Reglamento de desarrollo de la LOPD establece la obligación de realizar una auditoría de cumplimiento de estas medidas. Una de las primeras referencias que encontramos sobre la obligación de auditar se encuentra en la Instrucción 1/1995 de la Agencia Española de Protección de Datos, de 1 de marzo, relativa a la prestación de servicios de información sobre solvencia patrimonial y de crédito[194], estableciéndose en su cuarta norma que:

194 Agencia Española de Protección de Datos (1995). Instrucción 1/1995, de de 1 de marzo, de la Agencia Española de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y de crédito.

«(…) la implantación, idoneidad y eficacia de dichas medidas se acreditará mediante la realización de una auditoría, proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y la remisión del informe final de la misma a la Agencia de Protección Datos».

No obstante, esta obligación se aplicaba exclusivamente a aquellos sistemas que almacenasen o procesasen información relativa al cumplimiento o incumplimiento de las obligaciones dinerarias de acuerdo a lo establecido en el artículo 28 de la LORTAD. Con posterioridad, encontramos ya en la regulación que de esta obligación se realizaba en el artículo 17 del Reglamento de Medidas de Seguridad:

*«**Artículo 17. Auditoría.***

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos».

Podemos observar dos diferencias fundamentales con la regulación que de la obligación de auditar se realizaba en la Instrucción 1/1995:

- Se elimina la obligación de remitir el informe de auditoría a la Agencia Española de Protección de Datos.
- Se elimina la exigencia de someterse a una nueva auditoría tras la adopción de las medidas específicas que, en su caso, la Agencia determinara, en función de la revisión del informe.

Durante algunos años se planteó la duda de si el modelo de auditoría fijado en la Instrucción 1/1995 seguía vigente para los tratamientos relativos al cumplimiento de obligaciones dinerarias. En este sentido, la Memoria de la Agencia Española de Protección de Datos del año 1999 vino a zanjar dicho asunto:

«el contenido de ambas auditorias es similar de forma que el artículo 17.2 del Reglamento de Medidas de Seguridad no hace sino reiterar, para la totalidad de los ficheros sometidos al nivel medio de seguridad, en los términos establecidos en el artículo 4.2 del propio Reglamento lo que ya disponía el apartado quinto de la norma cuarta de la Instrucción 1/1995 (…)

En consecuencia, teniendo en cuenta que el Reglamento de Medidas de Seguridad es norma posterior, reguladora de la misma materia que la Instrucción 1/1995, en cuanto a los ficheros a los que se refiere el artículo 28 de la LORTAD, habrá de entenderse que la norma cuarta de la Instrucción ha sido derogada por el artículo 17 del Reglamento, siendo éste el que habrá de regir en lo sucesivo para todos los ficheros sujetos a medidas de seguridad de nivel medio, entre los que se encuentran la solvencia patrimonial y crédito de las personas físicas».

Más allá de las diferencias señaladas, podemos identificar los siguientes aspectos de la auditoría de medidas de seguridad exigida por el Reglamento de Medidas de Seguridad:

- La auditoría podrá ser interna o externa.
- Se llevará a cabo periódicamente, al menos cada dos años.
- Se revisará el cumplimiento del Reglamento de Medidas de Seguridad y de procedimientos e instrucciones vigentes a la fecha de la realización de la auditoría.
- Se emitirá un informe que contendrá los hechos y observaciones realizadas y que será analizado por el responsable de seguridad, que elevará sus conclusiones al responsable del fichero.

1.1 Obligación de auditar

En la actualidad, la obligación de auditar se encuentra recogida en el artículo 96 del Reglamento de desarrollo de la LOPD:

«1.A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas».

Podemos observar que la única modificación respecto al contenido del artículo 17 del Reglamento de Medidas de Seguridad es aquella que afecta al plazo establecido para la realización de la auditoría. En este sentido se prevé la realización de la auditoría con una mayor frecuencia de la marcada por el plazo de dos años, en función de que se produzcan modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas, reiniciándose, además, el cómputo de dos años, cuando se realice una auditoría por las causas enunciadas anteriormente.

La obligación de llevar a cabo una auditoría se completa con lo establecido por el artículo 110 del Reglamento de desarrollo de la LOPD en relación a los ficheros no automatizados:

«Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título».

Por tanto, se recoge expresamente la obligación de someter a los ficheros no automatizados a una auditoría de las medidas de seguridad aplicadas.

1.1.1 Alcance de la auditoría

En relación al alcance de la auditoría, podemos distinguir una obligación subjetiva y una obligación objetiva. En cuanto a la **subjetiva**, el artículo 9 de la LOPD hace recaer la obligación de adoptar las medidas de seguridad desarrolladas reglamentariamente en el responsable del fichero y, en su caso, en el encargado de tratamiento. A ambos se prohíbe expresamente registrar datos de carácter personal en ficheros que no reúnan las condiciones que se determinen en el Reglamento de desarrollo de la LOPD con respecto a la integridad y seguridad de los datos y por lo tanto, será su responsabilidad llevar a cabo la auditoría en los plazos previstos. Por otro lado, cuando nos referimos a la **obligación objetiva** de auditar los tratamientos de datos de carácter personal hacemos referencia al marco establecido por el Reglamento de desarrollo de la LOPD según el cual, deberán someterse a la auditoría todos los tratamientos de datos personales clasificados como de nivel medio y alto.

En este sentido, conforme a lo establecido por el artículo 81 Reglamento de desarrollo de la LOPD, la obligación afecta a aquellos tratamientos que contengan datos:

- Relativos a comisión de infracciones administrativas o penales.
- Relativos a la prestación de servicios de información sobre solvencia patrimonial y crédito.
- Responsabilidad de las Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- De los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- De los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.
- Responsabilidad de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
- De ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

- Recabados para fines policiales sin consentimiento de las personas afectadas.
- Derivados de actos de violencia de género.
- Responsabilidad de los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y de localización

No obstante, en relación al alcance de la auditoría, debemos tener en cuenta que la obligación contenida en el artículo 96 del Reglamento de desarrollo de la LOPD no implica única y exclusivamente la revisión de las medidas técnicas, sino que también alude al cumplimiento de medidas de tipo organizativo que incluyen procedimientos y controles de seguridad. En este sentido, los aspectos que serán objeto de auditoría, son los siguientes:

- ***Controles:*** Basándonos en la ISO 27000 serán controles las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. En otros casos, *control* es también utilizado como sinónimo de salvaguarda o contramedida. En línea con esta definición, debemos entender por *controles*, los mecanismos establecidos por el responsable del fichero o por el encargado del tratamiento para garantizar el cumplimiento de las obligaciones contenidas en el Reglamento de desarrollo de la LOPD.
- ***Procedimientos:*** Un procedimiento es la secuencia de acciones que se deberá seguir para obtener un determinado resultado. En concreto, definimos procedimiento como un documento escrito que refleja detalladamente las actividades de las que consta un proceso, es decir la forma específica de llevar a cabo las actividades y tareas propias de un proceso. El propio Reglamento de desarrollo de la LOPD dispone de forma expresa la obligación de desarrollar un procedimiento para el cumplimiento de las medidas de seguridad. Sin embargo, en otros casos, si bien el Reglamento de desarrollo de la LOPD no exige el desarrollo de un procedimiento, encontramos que se trata de la mejor forma para garantizar el cumplimiento de la obligación como por ejemplo los procedimientos que normalmente se elaborarán para la identificación en el acceso de los usuarios al Sistema de Información y que también deberá ser objeto de la auditoría.
- ***Medidas de seguridad.***

1.1.2 Tipos de auditoría previstas en la norma

Tal y como establece el artículo 96 del Reglamento de desarrollo de la LOPD, *los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una* ***auditoría interna o externa****.*

Por tanto, los responsables de ficheros tienen la posibilidad de cumplir con la obligación de auditar a través de dos vías:

- ***Auditoría interna:*** Si bien el Reglamento de desarrollo admite esta posibilidad, la misma no deja de presentar ciertos inconvenientes, ya que la realización de una auditoría por parte de los empleados de una organización podría adolecer de la independencia necesaria. No obstante si decide llevarse a cabo mediante esta vía es recomendable seguir las pautas recogidas en la Instrucción 1/1995 de la Agencia Española de Protección de Datos:
  - La auditoría deberá ser llevada a cabo por personal competente.
  - Deberá ser realizada por personal independiente de cualquier otro departamento interno o externo de la organización y en especial de aquellos departamentos relacionados con la gestión de los Sistemas de Información y la Seguridad.
  - Que el procedimiento siga criterios de imparcialidad, independencia y objetividad.
- ***Auditoría externa:*** La presente vía, en principio, ofrecerá mayores garantías de imparcialidad y especialización. En este sentido, y en relación con la selección de auditores externos, hay que hacer referencia a los criterios que se seguirán para su selección. El Reglamento de desarrollo de la LOPD no incluye ningún requisito específico respecto a las condiciones que deberán cumplir los auditores**,** siendo esta una de las cuestiones más polémicas respecto al cumplimiento de esta obligación. Del mismo modo que para los auditores de cuentas existe un censo oficial, no existe ningún censo ni certificación oficial que permita identificar a los profesionales que puedan realizar la auditoría de medidas de seguridad. Tampoco existen titulaciones oficiales en España en este sentido y esta ausencia de regulación, junto a la obligatoriedad de la auditoría establecida por el Reglamento de desarrollo de la LOPD, han dado lugar a la aparición de prestadores de servicios no cualificados que ofrecen a los responsables de ficheros auditorías que, en la mayoría de los casos, no les permitirán cumplir con sus obligaciones. La práctica diaria demuestra que muchas de estas auditorías las están realizando personas sin los conocimientos necesarios para evaluar y probar, con una mínima garantía. Por último, cabe destacar que existen organizaciones privadas que conceden títulos una vez acreditados conocimientos suficientes.

Se trata de títulos que si bien no están homologados a nivel oficial, si ofrecen una cierta garantía. En este sentido pueden citarse las certificaciones emitidas por ISACA[195]:

- **CISA**. Certificación de Auditoría de Sistemas de Información (*Certified Information System Auditor*).
- **CISM**. Certificación de Gerente de Seguridad de la Información (*Certified Information Security Manager*)

2. La realización de auditorias

Ni la normativa en materia de protección de datos de carácter personal ni la propia Agencia Española de Protección de Datos aportan una concreción sobre cómo se deben realizar las auditorías bienales marcadas por el Reglamento de Desarrollo de la LOPD. Por tanto, existe un vacío legal en este sentido que debe ser superado con la propia experiencia de la realización de auditorías en otros campos así como por el propio sentido común.

Por tanto, en este punto de nuestra exposición vamos a proceder a aportar una breve Guía que permita a todos los responsables del tratamiento cómo se debe ejecutar una auditoría en materia de protección de datos de carácter personal, ajustándonos a unos criterios de eficacia, eficiencia y legalidad, en este sentido, que permitan obtener un proceso y un informe final de auditorías de plenas garantías.

2.1 Fases de la auditoría

2.1.1 Identificación de los interlocutores

Nuestro primer paso consistirá en la designación de las personas o interlocutores que, a lo largo del proceso de auditoría, estará en contacto con el equipo auditor, facilitando el acceso a las áreas, sistemas y responsables definidos. En función del tamaño de la organización y del volumen de la información o de los sistemas a auditar, es altamente recomendable designar un comité o equipo de trabajo.

195 *Information Systems Audit and Control Association* (www.isaca.org)

En todo caso, tanto si hablamos de interlocutores como si hablamos de un comité o equipo de trabajo, éstos deberán asumir las siguientes responsabilidades:

- Mantenimiento de la comunicación con el equipo auditor.
- Garantizar que, a nivel interno, no existirán trabas para la realización de las tareas a desarrollar.
- Facilitar la documentación requerida

2.1.2 Definición del alcance

Una vez designados los interlocutores o, en su caso, el equipo de trabajo, será necesario concretar el alcance de la auditoría. Como regla general, el alcance ya habrá sido definido, al menos, sus aspectos más básicos, sobre todo si tenemos en cuenta que muchas auditorías se realizan de forma externa, es decir, a través de terceras entidades, distintas al responsable del fichero o tratamiento. No obstante, es habitual que el alcance no se detalle completamente en las fases previas y por lo tanto será necesario que, de acuerdo con los interlocutores o el equipo de trabajo designado, se lleve a cabo la definición de cuáles van a ser las y/o procesos de negocio incluidos en la auditoría así como la identificación de los recursos de información a auditar

2.1.3 Elaboración de un calendario de actuaciones

Una vez detallado el alcance, pueden establecerse con garantías las actuaciones que será necesario llevar a cabo para el correcto desarrollo de la auditoría. Es fundamental en este sentido marcar plazos concretos para la realización de todas y cada una de las fases, cerrando fechas para reuniones, entrevistas y visitas a las instalaciones. De esta forma se evitan retrasos indeseados y se garantiza que entre las distintas actuaciones no se deja pasar un excesivo plazo de tiempo que pueda afectar al buen devenir de la auditoría. Por tanto, es altamente recomendable dejar cerradas las siguientes fechas:

- Inicio de los trabajos.
- Fecha para la recogida de la información inicial solicitada.
- Fechas para la realización de entrevistas.
- Visitas a las instalaciones.
- Fecha de entrega del primer borrador de informe de auditoría.

- Fecha de entrega del informe definitivo de auditoría.

Asimismo, es conveniente hacer entrega al auditado del calendario de actuaciones y, a ser posible, darle la categoría de compromiso entre ambas partes.

2.1.4 Recogida de información

Núcleo central y del cual depende el éxito de la auditoría. Se define desde el inicio de la auditoría hasta la entrega del primer borrador de informe de auditoría. En el momento del inicio del proyecto, deberá solicitarse la información que el auditor estime necesaria para la preparación de la auditoría y que se compondrá fundamentalmente de:

- El Documento de Seguridad.
- Documentación relativa al registro de los ficheros ante el Registro de la Agencia Española de Protección de Datos.
- Organigrama de la entidad.
- Listado de sedes e instalaciones.
- Mapa de los Sistemas de Información.
- En su caso, los informes de auditorías realizados con anterioridad.
- Cualesquiera información que pueda servir para identificar y comprender la actividad de la organización a auditar.

La forma de recabar toda la información, anteriormente citada, es variopinta:

- Entrevistas y reuniones.
- Visitas a las instalaciones.
- Documentación.
- Análisis de las páginas web de la entidad así como de su Intranet.
- Auditoría de sistemas de información.

En este sentido es recomendable llevar un registro de la documentación solicitada y entregada, de forma que en el informe puedan reverenciarse las evidencias en las que se basan las observaciones,

recomendaciones y no conformidades. El registro debería incluir toda la información relevante e incluir sobre cada uno de los documentos entregados:

- Identificación.
- Fecha de solicitud.
- Fecha de entrega.
- Persona que entrega el documento.
- Tipo de documento.
- Versión.
- Observaciones.
- Cuando no se pueda acceder a la documentación requerida, se deberá hacer constar tal circunstancia tanto en el registro como en el informe final de auditoría.

2.1.5 Análisis de la información

El análisis de toda la información recabada, debe permitir determinar el grado de cumplimiento de las medidas de seguridad exigidas por el Reglamento de desarrollo de la LOPD. Dicho análisis debe basarse en el estudio detallado de la información obtenida de forma que se obtenga una visión completa del estado de la entidad. Los incumplimientos detectados deben basarse en la información obtenida durante la auditoría y por ello, para cada aspecto auditado, debe indicarse:

- Obligación contenida en el Reglamento de desarrollo de la LOPD.
- Estado actual del auditado, en relación con las evidencias recogidas.
- Valoración del grado de incumplimiento y del riesgo que dicho incumplimiento implica para el auditado.
- Recomendaciones.
- Acciones de mejora.

2.1.6 Elaboración y presentación del informe

Finalmente el equipo auditor procederá a elaborar el informe de auditoría y proceder a su entrega, junto a toda la documentación utilizada, al responsable de seguridad que posteriormente elevará las

conclusiones al responsable del fichero con el objeto de que la entidad adopte las medidas necesarias para subsanar los incumplimientos detectados.

2.2 Metodología

No existen procedimientos o metodologías avaladas de forma general, lo que deriva en una gran variedad de enfoques a la hora de afrontar el proyecto, lo cual se refleja en los diversos tipos de informes que podemos encontrar. En este sentido podemos seguir el análisis de Marzo y Macho-Quevedo[196] y propondremos las dos metodologías más extendidas en el ámbito de la Seguridad de la Información: el estándar de seguridad desarrollado por ISO y al propuesto por la ISACA.

2.2.1 Estándar ISO/IEC

La ISO 27002 surgió como un estándar para la Seguridad de la Información y fue publicado por primera vez como ISO/IEC 17799:2000 por la *International Organization for Standardization* -ISO- y por la *International Electrotechnical Commission* -IEC-, en el año 2000 con el título de *Information technology - Security techniques - Code of practice for information security management*.

Se trata de un estándar que proporciona recomendaciones de las mejores prácticas para la gestión de la Seguridad de la Información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la Seguridad de la Información. Su contenido se basa en 39 Objetivos de Control, que en total abarcan 133 Controles que se encuentran agrupados en once Dominios:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.

196 MARZO PORTERA, A. y MACHO-QUEVEDO, A. (2004): *La Auditoría de Seguridad en la Protección de Datos de Carácter Personal.* Ediciones Experiencia. Barcelona.

- Desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad de negocio.
- Conformidad.

2.2.2 COBIT

Estos objetivos fueron publicados por la ISACA por primera vez en 1996. Se trata de una serie de objetivos de control para la información y Tecnologías relacionadas. Es un conjunto de mejores prácticas para el manejo de información creado por la ISACA y el Instituto de Administración de las Tecnologías de la Información -*IT Governance Institute*- en 1992. La primera edición fue publicada en 1996.

COBIT tiene 34 objetivos de alto nivel que cubren 318 objetivos de control -específicos o detallados- clasificados en cuatro dominios:

- Planificación y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Supervisión y Evaluación.

3. El informe de auditoría

3.1 Contenido del informe

El informe de auditoría, tal y como establece el artículo 96 Reglamento de desarrollo de la LOPD, deberá atenerse a los siguientes requisitos:

- Deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario.
- Identificará las deficiencias detectadas. Para cada una de estas deficiencias o incumplimientos, se dictará una No-Conformidad en el informe.

- Propondrá las medidas correctoras o complementarias necesarias.
- Incluirá todos los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

De forma adicional, podrán incluirse en el informe otros datos que aumenten su utilidad para el auditado, como pueden ser los siguientes:

- **Detalle de riesgos y sanciones.** En función de las deficiencias detectadas, el auditor podrá advertir del riesgo concreto en el que se está incurriendo.
- **Otras recomendaciones.** El Reglamento de desarrollo de la LOPD exige que el informe incluya las medidas correctoras necesarias para adecuar al auditado a lo dispuesto por la norma. Asimismo, el auditor podrá proponer otras recomendaciones destinadas a facilitar la gestión de la información auditada y el cumplimiento de las obligaciones del responsable. Dichas recomendaciones pueden referirse a:
  - Elaboración de un Plan de Formación del personal que tiene acceso a datos de carácter personal, de forma que se facilite la implantación de medidas de seguridad y la detección de posibles incumplimientos en el futuro.
  - Establecimiento de controles adicionales.
  - Establecimiento de un Plan de Contingencia o recuperación frente a

3.2 Análisis

Tal y como establece el artículo 96.3 del Reglamento de Desarrollo de la LOPD, los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas.

Esta previsión ha sido criticada por algunos autores que esperaban una modificación de una obligación que ya estaba contenida en el artículo 17 del antiguo Reglamento de Medidas de Seguridad y que entienden que la figura del responsable de seguridad no es la más adecuada para constituirse en destinatario del informe, ya que el mismo contiene la evaluación de su labor.
En este sentido Touriño Expresa[197]:

197 TOURIÑO TROITIÑO, M. (2007): *Datos de Carácter Personal - Medidas de protección para ficheros automatizados en el borrador del Reglamento de la Ley 15/99*. Revista Datos Personales de 28 Julio 2007.

«Sin embargo, este apartado indica que "los informes de auditoria serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento". Es decir, otra vez: ¿juez y parte? (…) Ha sido una oportunidad perdida no haber reflejado las explicaciones de la Instrucción 1 de 1995, sobre el auditor y la auditoría».

No obstante, parece que la norma se inclina por la opción que parece más práctica desde el punto de vista de la implantación de las recomendaciones y de las acciones identificadas para cada No-Conformidad. Por otra parte, no debemos olvidar que el Reglamento de desarrollo de la LOPD, en su artículo 95, indica*:*

«En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento»

3.3 El informe de auditoría y la Agencia Española de Protección de Datos

El artículo 96.3 indica que los *informes deberán quedar a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.*

Por lo tanto, la Agencia Española de Protección de Datos no tiene por misión homologar los informes de auditoría elaborados a instancias de los responsables del tratamiento y de hecho quiso zanjar este asunto en un informe incluido en la Memoria de 1999[198]:

«(…) El artículo 17 dispone, junto con la obligación general de someter los sistemas e instalaciones a auditoría y el contenido de ésta que "los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos".

De ello se desprende que, una vez elaborado el informe de auditoría, deberán comunicarse sus resultados, adoptándose las medidas pertinentes, sin que ello exija una "aprobación" formal y

198 Agencia Española de Protección de Datos. Memoria 1999 [en línea]. Disponible en: http://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2003/common/pdfs/MemoriaApd1999.pdf

externa de su contenido, que no habrá de ser remitido a la Agencia Española de Protección de Datos, sino "puesto a su disposición".

Ello supone que será el responsable del tratamiento, siguiendo las recomendaciones del responsable de seguridad quien habrá de implantar las medidas precisas, derivadas del informe, de forma que, en caso de no implantarse y no cumplirse los requisitos de seguridad establecidos en el Reglamento, incurrirá en responsabilidad, constitutiva de infracción grave según el artículo 44.3 h) de la LOPD, lo que se comprobará por esta Agencia Española de Protección de Datos a través del examen, en su caso, del informe de auditoría y de la implantación efectiva de las medidas requeridas».

Por tanto, solo deberá entregarse el informe de auditoría en caso de un requerimiento de la Agencia Española de Protección de Datos o de las agencias autonómicas competentes que podrán solicitarlo en el ejercicio de la potestad de inspección que les confiere la LOPD. En este punto podemos citar una resolución de archivo de actuaciones de la Agencia de Protección de Datos de la Comunidad de Madrid. En este caso, la Agencia de Protección de Datos de la Comunidad de Madrid había requerido los informes de auditoría a los responsables del tratamiento de la Administración de la Comunidad de Madrid durante el primer semestre del año 2006. Dicho requerimiento se realizó en el marco de un Plan de Auditorías que la Agencia de Protección de Datos de la Comunidad de Madrid realiza con carácter anual entre los responsables del tratamiento sujetos al control de la agencia autonómica y que hayan cumplido con la obligación de auditar en el año anterior.

La Subdirección General de Inspección y Tutela de Derechos abrió un expediente de actuaciones previas contra aquellos responsables de fichero que no habían enviado las citadas auditorías, otorgando tres meses improrrogables para el envío de las mismas. Puesto que dichos responsables finalmente enviaron las auditorías en el plazo referido anteriormente, se procedió a dictar una resolución de archivo de actuaciones previas de cada uno de los expedientes abiertos por la no remisión de las mismas:

«De las actuaciones practicadas por la Agencia de Protección de Datos de la Comunidad de Madrid ante el Hospital El Escorial de la Consejería de Sanidad y Consumo, con domicilio en Ctra. Guadarrama al Escorial, Km. 17,6, 28200 MADRID, que han dado lugar a la tramitación del expediente E/00/2006, y en base a los siguientes:

HECHOS

***PRIMERO**.- Según consta en el Registro de Ficheros de Datos de Carácter Personal de esta Agencia de Protección de Datos, el Hospital El Escorial de la Consejería de Sanidad y Consumo, en su calidad de responsable tiene inscritos los siguientes ficheros de datos de carácter personal, con nivel de seguridad alto, no existiendo, por parte de esta Agencia, constancia de que hayan sido sometidos a la auditoría bienal obligada para este tipo de ficheros:*

Nombre del fichero	*Código de inscripción*	*Nivel de medidas de seguridad*
..	199102...	ALTO
..	199102...	ALTO
..	199102...	ALTO
..	199102...	ALTO

***SEGUNDO**.- En fecha de 00/00/2006, la Agencia de Protección de Datos de la Comunidad de Madrid remitió al Hospital El Escorial requerimiento para que en el plazo de 3 meses, a partir de su recepción, se enviaran a este Organismo la auditoria de seguridad de los ficheros (…), en cumplimiento de lo previsto en la legislación sobre protección de datos, basando el referido requerimiento en la obligación que establece el artículo 17 del Real Decreto 994/1999, de 11 de junio, en relación con la remisión de las auditorias correspondientes a los ficheros de carácter personal de nivel medio y alto.*

***TERCERO**.- En fecha de 00/00/2006 tiene entrada, en el Registro de esta Agencia, escrito del Hospital El Escorial, en contestación al requerimiento descrito en el hecho anterior, adjuntando informe final de la auditoria correspondiente a los ficheros (…).*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia de Protección de Datos de la Comunidad de Madrid, conforme a lo dispuesto en el artículo 12.2 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid y en el artículo 10.1 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de las funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal , en relación con los artículos 41.1 y 37 g) de la Ley

Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

II

El artículo 11.1.j) del Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid, prevé que el Director de la Agencia de Protección de Datos de la Comunidad de Madrid tiene, entre sus funciones, la de recabar de los responsables de los ficheros bajo el ámbito de aplicación de la Ley 8/2001, de 13 de julio, la información necesaria para el cumplimiento de sus funciones.

El artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece que el responsable del fichero y, en su caso, el encargado del tratamiento deberán 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. Por su parte, el artículo 8. c) de la Ley 8/2001, de 13 de julio, de Protección de Datos en la Comunidad de Madrid, impone a los responsables de los ficheros la obligación de adoptar las medidas de seguridad a que se encuentre sometido el fichero de acuerdo a la normativa vigente.

El artículo 4 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter general, establece la aplicación de los niveles de seguridad en los siguientes términos:

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las

personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

El artículo 17 del mismo texto legal prevé la auditoría como una de las medidas de seguridad de nivel medio:

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Siendo la auditoría una de las medidas de seguridad de nivel medio, conforme a lo previsto en el artículo 4 trascrito, la auditoría es también una medida de seguridad aplicable a los ficheros de nivel alto.

Por tanto, y atendiendo a los preceptos jurídicos anteriores, los responsables de ficheros incluidos en el ámbito de actuación de la Agencia de Protección de Datos de al Comunidad de Madrid tienen la obligación de remitir a este Organismo, tras la oportuna solicitud, los informes de auditorías correspondientes a los ficheros de nivel medio y alto, obligación que, de acuerdo con la documentación remitida por el Hospital El Escorial de la Consejería de Sanidad y Consumo, puede constatarse cumplida en el plazo concedido tras el requerimiento que da inicio al expediente de referencia.

III

Visto el marco jurídico descrito y la documentación obrante en el expediente, debe procederse al archivo de las presentes actuaciones al no apreciarse vulneración de la legislación de protección de datos de carácter personal.

Vistos los preceptos citados y demás de general de aplicación,

El Director de la Agencia de Protección de Datos de la Comunidad de Madrid,

RESUELVE:

***PRIMERO**: DECLARAR el archivo de las presentes actuaciones.*

***SEGUNDO**: NOTIFICAR la presente resolución al Hospital El Escorial de la Consejería de Sanidad y Consumo de la Comunidad de Madrid.*

***TERCERO**: ADVERTIR al Hospital El Escorial de la Consejería de Sanidad y Consumo que contra esta resolución, que pone fin a la vía administrativa (artículo 14.3 de la Ley 8/2001, de 13 de julio, de Protección de Datos en la Comunidad de Madrid), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, según la redacción dada por la Ley 4/1999, de 13 de enero, que la modifica, podrá interponer potestativamente recurso de reposición ante el Director de la Agencia de Protección de Datos de la Comunidad de Madrid en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante los Juzgados de lo Contencioso Administrativo.*

EL REGLAMENTO DE DESARROLLO DE LA LOPD

I. ¿Por qué un nuevo Reglamento?

1. Introducción

El Reglamento de Medidas de Seguridad, predecesor del Reglamento de desarrollo de la LOPD, fue aprobado por el Real Decreto 994/1999, de 11 de junio, publicado en el Boletín Oficial del Estado de 25 de junio de 1999.

Dicha norma tenía como misión principal cumplir con la previsión del artículo 9 de la LORTAD, en el que se establecía la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativa que garantizasen la seguridad de los datos de carácter personal y evitaran su alteración, pérdida, tratamiento o acceso no autorizado.

Por tanto, se hacía necesario un desarrollo reglamentario adecuado, que permitiera a los responsables del tratamiento disponer de un marco de referencia para la implantación de las medidas de seguridad.

El Reglamento de Medidas de Seguridad, en su Exposición de Motivos, declara que su objeto es el desarrollo de lo dispuesto en la LORTAD:

«El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado».

No obstante, el Reglamento de Medidas de Seguridad, que había resultado adecuado en un principio para satisfacer unas necesidades concretas, se vio pronto afectado por la aprobación, a los pocos meses de su entrada en vigor, de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, que vino a sustituir a la LORTAD y cuyo ámbito de aplicación era sustancialmente más amplio que el de su predecesora.

El cambio de escenario requería, como reconoce el texto de la propia Ley Orgánica de Protección de Datos, de un desarrollo reglamentario acorde con las nuevas necesidades. Sin embargo, mientras dicho desarrollo tenía lugar, se mantuvo la vigencia del Reglamento de Medidas de Seguridad y de otras normas del mismo rango relacionadas, en tanto en cuanto no se opusieran a la LOPD.

El proceso de elaboración de este nuevo reglamento fue largo, y durante ese lapso de tiempo, la aplicación de la Ley Orgánica de Protección de Datos fue poniendo de manifiesto otros puntos necesitados de una mayor concreción y desarrollo. Así, por ejemplo, la aplicación de los principios contenidos en la Ley Orgánica de Protección de Datos hizo necesaria una regulación más detallada de dichos aspectos, carencia que hasta el año 2008 se ha suplido con la interpretación aportada por la Agencia Española de Protección de Datos.

El resultado final fue la publicación, el 19 de enero de 2008, del Real Decreto 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

2. De la LORTAD a la LOPD

2.1 La LORTAD

En 1992 se aprobó la primera Ley que cumplía el mandato recogido en el artículo 18.4 de la Constitución: la Ley Orgánica 5/1992, de 29 octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, comúnmente conocida como LORTAD y que era la respuesta del legislador al mandato contenido en el artículo 18.4 de la Constitución que limitaba el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. Así, la Exposición de Motivos de la LORTAD establecía:

«Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley».

En base a la citada Exposición de Motivos, la LORTAD dentro de su Título Segundo, dedicado a los principios de aplicación para la protección de los datos personales, enunciaba en su artículo 9, en relación a la seguridad de los datos:

«1. El responsable del fichero deberá 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.
2. No se registrarán datos de carácter personal en ficheros automatizados 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 automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley».

Quedaba de esta forma habilitado el desarrollo reglamentario, desarrollo que también era citado, aunque no de forma directa, en el artículo 43.3 h) de la propia LORTAD:

«3. Son infracciones graves: (…) h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria, se determinen».

En 1995, tres años después de la aprobación de la LORTAD, se promulgaba la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas en lo que respecta al tratamiento de los datos cuyo objetivo principal radicaba en establecer un marco de protección común de las libertades y de los derechos fundamentales y en particular del derecho a la intimidad, en lo que respecta al tratamiento de los datos de carácter personal. Su misión, hacer respetar el derecho a la vida privada, asegurar la libre circulación de datos dentro de la comunidad y evitar distorsiones de competencia entre empresas.

El legislador se encontró, por tanto, con la necesidad y la obligación de llevar a cabo la transposición de la Directiva al ordenamiento jurídico español, obligación que en un primer momento, se pretendió cumplir mediante la reforma de la propia LORTAD. En agosto de 1998, el Gobierno remitió al Parlamento un Proyecto de Ley de reforma parcial de la LORTAD que pretendía evitar el incumplimiento en el que finalmente incurrió España, del plazo de tres años establecido por el artículo 32.1 de la Directiva 95/46/CE para la transposición de la misma.

El contenido de la Directiva implicaba realizar importantes cambios dentro del marco jurídico español y dicha circunstancia influyó para que se considerara que era la ocasión adecuada para, además de recoger los aspectos más novedosos de la normativa europea, revisar algunos de los puntos necesitados de reforma en la LORTAD. No en vano, se habían interpuesto distintos recursos de inconstitucionalidad contra la LORTAD, que finalmente fueron resueltos con las sentencias de 30 de noviembre de 2000 y de las que ya hemos hablado en capítulos anteriores.

La necesidad de transposición de la Directiva por un lado y, de otra parte, la existencia de aspectos controvertidos en la LORTAD fueron los factores que detonaron el inicio del proceso de desarrollo y aprobación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Dicho esto, pocos meses antes de la aprobación de la Ley Orgánica de Protección de Datos, se publicaba en el Boletín Oficial del Estado, el Reglamento de Medidas de Seguridad que venía cumplir con la previsión de desarrollo de la LORTAD.

2.2 La Ley Orgánica de Protección de Datos

El contexto en el que se elaboró el anterior desarrollo reglamentario, estuvo marcado por la evolución en el marco de la protección de los datos personales que finalmente cristalizó en el paso de la LORTAD a la Ley Orgánica de Protección de Datos.

En este sentido, la Ley Orgánica de Protección de Datos, es una norma con un objeto mucho más amplio que el marcado por la LORTAD, tal y como se establece en su primer artículo:

«La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar».

La presente definición, de la que desaparece la referencia al artículo 18.4 de la Constitución Española, va incluso más allá del objeto establecido por la propia Directiva 95/46/CE, que únicamente referencia, en su primer artículo, una protección reforzada de la intimidad en lo que atañe al tratamiento de los datos de carácter personal:

«Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales».

El artículo 1 de la LOPD, amplía esta protección al honor y en un sentido más general, a la intimidad familiar incluso, de forma previa a las Sentencias del Tribunal Constitucional 290 y 292 del año 2000 que finalmente reconocieron el derecho a la protección de datos personales como un derecho fundamental de carácter autónomo.

En lo relativo al ámbito de aplicación, el artículo 2.1 de la LOPD establece:

«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».

De esta forma y, de acuerdo con las previsiones comunitarias, el ámbito de aplicación se extiende a cualquier tipo de tratamiento de datos personales, no limitándolo a los tratamientos automatizados. Por tanto, podemos observar que la LOPD nacía con una amplia vocación de generalidad cubriendo aspectos no previstos por la propia LORTAD.

Por otro lado, si nos referimos a los principios de protección de datos que deben ser respetados en cualquier tratamiento de datos personales, estos se recogen en el Título II de la LOPD y son los siguientes:

- Calidad de los datos.
- Derecho de información en la recogida de datos.
- Consentimiento del afectado.
- Datos especialmente protegidos.
- Seguridad de los datos.

- Deber de secreto.
- Comunicación de los datos.
- Acceso a datos por cuenta de terceros.

Durante la definición de estos principios, la Ley Orgánica de Protección de Datos se remite en dos ocasiones al desarrollo reglamentario, en concreto en los artículos 4 y 9 relativos al principio de calidad de los datos y al principio de seguridad respectivamente.

Más allá de estas dos remisiones, la práctica de los años de aplicación de la Ley Orgánica de Protección de Datos, puso de manifiesto que la regulación que de todos ellos hace, precisaba de un desarrollo más completo, que definiera con exactitud cuáles son las obligaciones que el cumplimiento de estos principios imponía a los responsables del tratamiento. Dicha circunstancia, unida a una falta de desarrollo que dejaba el campo abierto a la interpretación, se veía agravada, además, por la falta de Exposición de Motivos de la Ley Orgánica de Protección de Datos, hecho este que ya llamó la atención en el momento de su aprobación ya que fue eliminada en las últimas fases[199]:

«Posiblemente uno de los cambios más significativos que se aprecia en la nueva Ley orgánica 15/99 sea la ausencia de una breve Exposición de Motivos que sirva para justificar e introducir el sentido y transcendencia de la nueva regulación sobre protección de datos. Y ciertamente resulta llamativo por cuanto que el texto del proyecto de ley orgánica de modificación de la LORTAD sí se detenía a realizar una sencilla introducción del sentido de la nueva Ley».

La ausencia de Exposición de Motivos facilitó que los responsables del tratamiento no contaran ni tan siquiera con una pauta que señalara las líneas generales de actuación, en una materia de vital importancia como es la protección de un derecho de carácter fundamental, el derecho a la protección de los datos de carácter personal.

199 HERRÁN ORTIZ. A.: (2002) *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales.* Editorial Dykinson. Madrid.

2.3 Desarrollo y régimen transitorio

Al hablar del desarrollo reglamentario de la Ley Orgánica de Protección de Datos, no podemos obviar la habilitación contenida en su Disposición Final Primera:

«El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley».

Sin embargo, con el fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos de carácter personal, el legislador declaraba subsistentes, en la Disposición Transitoria Tercera de la Ley Orgánica de Protección de Datos, y «*hasta tanto se lleven a efectos las previsiones de la Disposición Final Primera»*, las normas reglamentarias existentes y, en especial, los Reales Decretos:

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

Por otro lado, la Disposición Adicional Primera de la Ley Orgánica de Protección de Datos dispone, para los ficheros de datos personales no automatizados, un plazo para su adecuación de «*doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados».*

Se establecía de esta forma un marco transitorio en espera del necesario desarrollo, y mediante el cual las normas citadas, y entre ellas, el Reglamento de Medidas de Seguridad, se mantenían en vigor al tiempo que se marcaba un límite temporal que finalmente se prolongó más allá de los plazos marcados inicialmente.

3 La LOPD y el Reglamento de Medidas de Seguridad

3.1 Necesidad de desarrollo de los principios de la LOPD

El Título Segundo de la Ley Orgánica de Protección de Datos establece los principios fundamentales del derecho a la protección de los datos de carácter personal. No obstante, dichos principios no se encuentran desarrollados, por completo, dentro del articulado de la Ley Orgánica.

La aplicación práctica de la Ley Orgánica ha presentado numerosas dificultades sobre todo en todo aquello relativo a la aplicación de los propios principios en la materia y sobre los que es necesario, en este punto de nuestra exposición, detenerse.

3.1.1 Calidad de los datos

Tal y como establece el artículo 4.3 de la Ley Orgánica de Protección de Datos de Carácter Personal:

«los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado».

Sin embargo, ¿qué medidas deberá tomar el responsable de tratamiento para garantizar el cumplimiento de este principio? La Directiva 95/46/CE, en su artículo 6 d) mencionaba al respecto:

«Los Estados miembros dispondrán que los datos personales sean: (…) d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados».

Por contra, la Ley Orgánica de Protección de Datos de Carácter personal no recoge ni tan siquiera la alusión a las *«medidas razonables»* realizada en la propia Directiva europea. Nuestro sistema legislativo exigía un correcto desarrollo que estableciese qué medidas era necesario adoptar en aquellos casos en los que los datos sean inexactos o no reflejen con veracidad la situación del titular de los mismos. De lo contrario sería posible encontrar situaciones o casuísticas en las que los

responsables del tratamiento tuviesen una exigencia desproporcionada en el mantenimiento exacto y actualizado de los datos de carácter personal.

Asimismo, el artículo 4.5 de la Ley Orgánica contiene otra habilitación para el desarrollo reglamentario:

«Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento integro de determinados datos».

3.1.2 Información

El presente principio, se encuentra recogido en el artículo 5 de la Ley Orgánica que, establece una serie de puntos sobre los que cualquier entidad que trate datos de carácter personal, deberá informar al interesado o afectado.

Como ya hemos tenido oportunidad de ver, nos encontramos con uno de los pilares básicos de la materia que nos ocupa y, tal y como declara el Tribunal Constitucional en su Sentencia 292/2000:

«sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (artículo 5 de la LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales (…) es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales...».

Como podemos observar el artículo 5 de la Ley Orgánica de Protección de Datos establece con bastante detalle las obligaciones que el responsable de tratamiento debe asumir. No obstante, quedaban pendientes algunos aspectos a considerar como la forma de acreditación del cumplimiento del principio de información o las obligaciones de información en supuestos especiales como la modificación del responsable del fichero.

3.1.3 Consentimiento

El artículo 6 de la Ley Orgánica de Protección de Datos exige que el consentimiento del afectado se produzca de forma inequívoca para cualquier tratamiento de datos personales, salvo que la ley disponga otra cosa. Dicho artículo también reconoce el derecho de oposición, cuando al hablar del consentimiento del afectado establece:

«En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal».

Sin embargo, la Ley Orgánica deja pendientes de desarrollo otros muchos aspectos. La imposibilidad de acreditar la obtención adecuada del consentimiento para los tratamientos llevados a cabo es uno de los motivos más frecuentes de sanción por parte de la Agencia Española de Protección de Datos, y en muchas ocasiones, existen supuestos en los que el responsable del tratamiento debe realizar un gran esfuerzo interpretativo de la Ley. Es el caso, entre otros, del consentimiento prestado por menores de edad, de la aplicación de las excepciones recogidas en el artículo 6 de la Ley Orgánica, o del procedimiento establecido para la revocación. Se trata por lo tanto de una de las materias en las que el desarrollo efectuado por el nuevo reglamento era más necesario.

3.1.4 Encargado del Tratamiento

Se encuentra regulada en el artículo 12 de la Ley Orgánica de Protección de Datos, regulación que, aun siendo extensa no abarca toda la casuística de esta figura, tal y como ha demostrado la aplicación práctica de la Ley ya que es bastante común la aparición de supuestos que no están convenientemente regulados, y que dejan abierta la posibilidad de diversas interpretaciones que, como en el caso de la obtención del consentimiento, devienen a menudo en incumplimientos y sanciones. El caso más frecuente en este sentido es el de la subcontratación por el encargado de tratamiento de servicios a terceros.

3.1.5 Seguridad de los datos

El principio de seguridad de los datos se encuentra recogido en el artículo 9 de la Ley Orgánica de Protección de Datos que, todo sea dicho, no observa el coste económico como una variable a la hora de establecer el nivel de protección del que deben gozar los datos en función de su naturaleza. Cosa que si hace, por contra, la Directiva europea en su artículo 17:

«Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse».

No obstante la Ley Orgánica de Protección de Datos sí establece en su artículo 9.3 una remisión expresa al desarrollo reglamentario:

«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».

3.2 Medidas de seguridad

La implantación de medidas de seguridad es uno de los aspectos en los que la necesidad de un desarrollo reglamentario era más que evidente. En este sentido, el Reglamento de Medidas de Seguridad ha servido a lo largo de todo su periodo de vigencia como referencia única a nivel normativo en la aplicación de medidas de seguridad y la experiencia de su aplicación ha permitido identificar las dificultades a las que se deben enfrentar los responsables de los tratamientos y que pasamos a detallar a continuación.

3.2.1 Atribución de los niveles de seguridad

A pesar de que la atribución de los niveles de seguridad aplicables a cada fichero que el Reglamento de Medidas de Seguridad llevaba a cabo en su artículo 4 eran adecuadas en función de la naturaleza de los datos, en algunos casos, estas reglas imponían un nivel de obligaciones a los responsables de los tratamientos que hacían muy difícil, por no decir imposible, su aplicación, sobre todo cuando nos encontrábamos en presencia de datos relativos a la salud o a la afiliación sindical y que suponía

la aplicación de medidas de nivel alto a los ficheros de recursos humanos. Obligación, a todas luces, desproporcionada para la mayoría de las organizaciones que no se encuentran, fundamentalmente por asuntos económicos, en disposición de cumplir con todos los requisitos que exigía el antiguo Reglamento de Medidas de Seguridad.

Sobre la base de la atribución de los niveles de seguridad del Reglamento de Medidas de Seguridad, se ha planteado a lo largo de estos años la necesidad de realizar algunas modificaciones de acuerdo con nuevas prácticas y supuestos que reclamaban la aplicación de niveles de protección adecuados.

3.2.2 Evolución

En lo relativo a las medidas de seguridad contenidas en el Reglamento de Medidas de Seguridad, su aplicación ha puesto de manifiesto algunos puntos que era conveniente revisar: cuestiones como las relacionadas con el control de acceso, la gestión de los soportes que contengan datos personales o la identificación y la autenticación requerían una revisión, sobre todo desde el punto de vista práctico.

3.2.3 Adecuación de las obligaciones formales

La práctica también ha puesto de manifiesto la existencia de aspectos a mejorar en lo que se refiere a las medidas de carácter organizativo. En primer lugar, se hacía necesaria una ordenación que contemplase con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad.

Además, se hacía necesario regular las obligaciones formales de forma que se contemplen las múltiples formas de organización material y personal de la seguridad de la información que se dan en la práctica en las entidades de nuestro país.

3.2.4 Medidas de seguridad de aplicación a los ficheros no automatizados

Es esta una de las mayores novedades acaecidas desde la entrada en vigor del Reglamento de desarrollo de la LOPD. Si bien, antes de la entrada en vigor del Reglamento de desarrollo de la LOPD, existía la obligación de adecuar estos tratamientos a lo establecido por la Ley Orgánica de Protección de Datos, el Reglamento de Medidas de Seguridad no preveía el establecimiento de medidas de seguridad concretas a tratamientos no automatizados y por ello, estos quedaban fuera

del ámbito normativo no existiendo un marco claro de actuación.

3.3 El Reglamento y la Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos, con el devenir de los años, se ha visto afectada por la evolución del marco normativo. Por tanto, su situación también requería un desarrollo reglamentario que el Reglamento de Desarrollo de la LOPD ha venido a completar sobre todo desde el punto de vista de su ámbito competencial así como de los procedimientos llevados a cabo ante la Agencia Española de Protección de Datos.

3.3.1 Ámbito competencial

En los últimos años se ha venido produciendo una evolución en el marco normativo que afecta, de forma directa, a la Agencia Española de Protección de Datos, siendo necesario que la misma abarque funciones adicionales.

En primer lugar, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, también conocida como LSSI, cuando regula las competencias sancionadoras en su ámbito de regulación, establece, en su artículo 43:

«Artículo 43. Competencia sancionadora.
1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.
No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta ley corresponderá al órgano que dictó la resolución incumplida.
Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta ley".

Podemos observar, por tanto, que la LSSI realiza una atribución directa de competencias en el ámbito sancionador en los siguientes supuestos:

7. El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 de la LSSI.
8. El incumplimiento de la obligación del prestador de servicios establecida en el artículo 22.1 LSSI, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.
9. El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas por el artículo 22.2 LSSI.

Asimismo, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, ha atribuido también competencias adicionales a la Agencia Española de Protección de Datos en materia sancionadora en su artículo 53:

«La competencia sancionadora corresponderá: (…)
b. A la Agenda de protección de Datos, cuando se trate de las infracciones muy graves comprendidas en el párrafo z del artículo 53 y de las infracciones graves previstas por el párrafo y del artículo 54».

Estos supuestos se refieren a infracciones graves y muy graves en materia de derecho de los consumidores y usuarios finales en relación con sus datos de tráfico y de incumplimiento de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de Conservación de Datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación[200]:

*«**Artículo 8. Protección y seguridad de los datos.***
1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no

200 Jefatura del Estado. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Publicado en el Boletín Oficial del Estado n.º 251 de 19 de octubre de 2007.

autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.
2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo».

Por tanto, todas estas competencias atribuidas a la Agencia Española de Protección de Datos requerían también de un desarrollo reglamentario que se ha recogido en el Reglamento de desarrollo de la LOPD.

3.3.2 Procedimientos tramitados por la Agencia

Como hemos apuntado anteriormente, existía la necesidad de desarrollar los procedimientos tramitados por la Agencia Española de Protección de Datos, y especialmente, el ejercicio de la potestad sancionadora. A esta regulación se ha dedicado el Título IX del reglamento -Procedimientos tramitados por la Agencia Española de Protección de Datos- en el que se ha optado por regular, en exclusiva, aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia Española de Protección de Datos, de las normas generales previstas para los procedimientos establecidos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al reglamento.

4 La elaboración del nuevo Reglamento

El proceso de elaboración del Reglamento fue un proceso largo y en el que se han tenido en cuenta las aportaciones de diferentes entidades, organismos y empresas implicados en distintos aspectos de la gestión de datos de carácter personal. Corresponde, en este punto, conocer cuáles han sido las necesidades y opiniones que han intervenido en la redacción del texto.

4.1 Primera versión

La primera versión del Reglamento, de 26 de noviembre de 2006, carecía de parte expositiva y constaba de 154 artículos, agrupados en nueve títulos, una disposición adicional única -*«Productos de software»*- y una disposición transitoria única -*«Plazos de implantación de las medidas de seguridad»*-.

Fue remitida para informe a la Secretaría General Técnica de los Ministerios del Interior, Cultura, Economía y Hacienda y Fomento y a la Dirección General para el Desarrollo de la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio y fue sometida a la consideración de la Agencia Española de Protección de Datos.

Se llevó a cabo una fase de consulta que derivó en numerosos informes:

- **Informe de 19 de enero de 2007 de la Secretaría General Técnica del Ministerio de Cultura:** El informe recoge diversas observaciones de índole material y formal. Entre las primeras, se considera que ha de armonizarse el Reglamento con otras disposiciones en proyecto, como la Ley para el acceso electrónico de los ciudadanos a las Administraciones públicas, y que debe procederse a la revisión de ciertos aspectos de su Título IX.
- **Informe de 23 de marzo de 2007 de la Secretaría General Técnica del Ministerio del Interior:** Pone de manifiesto las dificultades que pueden suponer diversas previsiones, como las medidas de seguridad aplicables a los ficheros no automatizados, para las Fuerzas y Cuerpos de Seguridad del Estado. Por ello, propone la ampliación de los plazos fijados en la disposición transitoria segunda para la implantación de las aludidas medidas en los ficheros policiales y el establecimiento de mecanismos de colaboración entre los órganos judiciales y las Fuerzas y Cuerpos de Seguridad para proceder a la puntual cancelación de los antecedentes policiales.

- **Informe sin fechar de la Dirección General para el Desarrollo de la Sociedad de la Información:** Sugiere volver a considerar el nivel alto de medidas de seguridad que se exige en el artículo 78 del Reglamento a los datos de tráfico y de localización, frente al exigido en el régimen del Real Decreto 994/1999, que establecía el nivel medio, y en el propio Reglamento para los datos relativos a infracciones administrativas o penales, nivel medio. Se critica, en esta línea, la ausencia en el expediente de justificación de ese nivel de exigencia y se sugiere dar trámite de audiencia en el procedimiento de elaboración del Proyecto a las entidades que puedan verse afectadas por esa previsión.
- **Informe de 20 de febrero de 2007 de la Dirección General de Telecomunicaciones y Tecnologías de la Información**
- **Informe de 17 de enero de 2007, de la Agencia Española de Protección de Datos.** Se trata del informe previsto en el artículo 37.1 h) de la Ley Orgánica de Protección de Datos y el artículo 5. b) del Estatuto de la Agencia Española de Protección de Datos aprobado por Real Decreto 428/1993, de 26 de marzo. En el mismo, la Agencia Española de Protección de Datos valora positivamente el texto normativo sometido a su consideración, sin perjuicio de lo cual formula numerosas observaciones, la mayoría de las cuales, tanto formales como sustantivas, han sido incorporadas, en mayor o menor medida, al proyecto.

4.2 Segunda versión del Proyecto

Teniendo en cuenta las modificaciones propuestas, con fecha de 30 de abril de 2007 se dio a conocer una segunda versión del proyecto, que constaba de un preámbulo, un artículo único, por el que se aprueba el Reglamento de desarrollo de la LOPD y una disposición derogatoria. A continuación, disponía de un índice del Reglamento y su parte dispositiva, integrada por 154 artículos, organizados en nueve títulos. La parte final del Reglamento estaba constituida por una disposición adicional y cuatro disposiciones transitorias.

Esta versión fue remitida para alegaciones a numerosas entidades y organismos, entre las que se encontraban:

- Consejo de Consumidores y Usuarios, Federación Española de Municipios y Provincias (FEMP).
- Consejo General de la Abogacía Española.
- Colegios y Asociaciones Profesionales.

- Sindicatos.
- Organizaciones Empresariales y Cámaras de Comercio.
- Asociación Española de Banca (AEB).
- Confederación Española de Cajas de Ahorro (CECA).
- Asociación Empresarial del Seguro (UNESPA).
- Federación Española de Comercio Electrónico y Marketing Directos (FECEMD).
- Autocontrol: Asociación para la autorregulación de la comunicación comercial
- Empresas de Tecnologías de la Información y las Telecomunicaciones.
- Asociaciones de Empresas de Consultoría y Calidad.
- Entidades y Asociaciones de Artistas, Intérpretes, Ejecutantes, y Sociedades de Gestión.
- Consejo de Coordinación Universitaria.
- Comisión de Libertades e Informática (CLI).
- Asociaciones de Archiveros, Bibliotecarios, Museólogos y Documentalistas.
- Asociaciones de Usuarios (AUTELSI).
- Consejo General del Notariado de España
- Colegio de Registradores de la Propiedad y Mercantiles de España.
- Autoridades de control autonómicas.

Muchas de estas empresas y asociaciones presentaron alegaciones, entre las que se pueden destacar:

- **Informe de 29 de mayo de 2007, de la Agencia Catalana de Protección de Datos:** Centra sus observaciones en la necesidad de que el Reglamento incorpore mayores referencias a las autoridades autonómicas de control en aquellos preceptos en que se regulan funciones y competencias de la Agencia Española de Protección de Datos: códigos tipo, transferencias internacionales de datos, procedimientos de la Agencia Española de Protección de Datos, entre otras.
- **Informe de 4 de junio de 2007, de la Agencia de Protección de Datos de la Comunidad de Madrid:** Incluye observaciones sobre numerosas materias reguladas en el proyecto. Exponen las razones que motivan su oposición a las definiciones de ficheros de titularidad pública y privada contenidas en el artículo 5 del Reglamento y a la regulación de los datos de las personas fallecidas. También formula numerosas consideraciones sobre la necesidad de que se incorporen previsiones que garanticen la coordinación entre el Registro General de Protección de Datos y los registros creados por las autoridades autonómicas de control y la actuación de éstas y la Agencia Española de Protección de Datos. Asimismo se señala la conveniencia de que se incluya una disposición final sobre la entrada en vigor y se formulan

varias observaciones a la parte dispositiva del Reglamento.

- **Informe de 18 de junio de 2007, de la Agencia Vasca de Protección de Datos:** El presente informe se centra en los fundamentos constitucionales de la reglamentación en proyecto, examinando la jurisprudencia constitucional en materia de desarrollo de los derechos fundamentales y la cláusula del artículo 149.1.1 de la Constitución. En su examen del contenido del Reglamento se exponen las dudas sobre la suficiencia del rango de la norma examinada para colmar las exigencias de ciertas cuestiones cuya regulación se aborda. También realiza algunas observaciones sobre la necesaria coordinación de competencias entre Agencia Española de Protección de Datos y las autoridades de control autonómicas.

4.3 Tercera versión

La tercera versión del Reglamento, de 12 de julio de 2007 consta de preámbulo, un artículo aprobatorio, cuatro disposiciones transitorias y una disposición derogatoria. Tras el índice del Reglamento de desarrollo, se incluye su parte dispositiva, integrada por 158 artículos, divididos en nueve títulos, y su parte final, integrada por una disposición adicional. Este texto fue remitido al Ministerio de Administraciones Públicas, a los efectos de la aprobación previa por el Ministro, prevista en el artículo 67.4 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

Finalmente, el 4 de septiembre de 2007, la Ministra de Administraciones Públicas realiza la aprobación previa del texto, aprobación llevada a cabo en base a lo establecido en el artículo 67.4 de la Ley de Organización y Funcionamiento de la Administración General del Estado. A dicha aprobación previa se adjuntan algunas observaciones específicas entorno a la propuesta de reforma de los artículos 11.3 y 24 del Reglamento y la sugerencia de añadir un precepto relativo al consentimiento en las solicitudes electrónicas dirigidas a las Administraciones públicas. Además, se realizan consideraciones adicionales sobre la distribución competencial en materia de protección de datos y su incidencia en el contenido del Reglamento. En este sentido, se establece una diferenciación entre el régimen contenido en los Títulos II a VIII del Reglamento, que contienen normas sustantivas, relacionadas con el contenido esencial del derecho fundamental a la protección de datos, y aspectos relativos al ejercicio del derecho que resultan decisivos en la configuración de su contenido, de conformidad con el artículo 149.1.1 de la Constitución. Frente a ello, el Título IX del Reglamento establece el régimen de los procedimientos tramitados por la Agencia Española de

Protección de Datos y, por tanto, sus preceptos no son aplicables a las autoridades autonómicas de protección de datos. Una vez realizada esa distinción, se propone introducir en el texto del Proyecto una disposición final en la que se invoque el título competencial en que se funda la aprobación de la norma proyectada. Se señala, no obstante, que algunas Comunidades Autónomas pueden promover controversias competenciales pues, como ha declarado el Tribunal Constitucional, dicho precepto *«no puede operar como una especie de título horizontal, capaz de introducirse en cualquier materia o sector del ordenamiento por el mero hecho de que pudieran ser reconducibles, siquiera sea remotamente, hacia un derecho o deber constitucional»*[201]. Por esta razón, se apunta el aludido riesgo y se recuerda que algunas Comunidades Autónomas, como las Islas Baleares o Aragón, han asumido funciones normativas sobre *«los ficheros de titularidad de las Administraciones públicas de la Comunidad Autónoma y los entes u organismos de cualquier clase vinculados o dependientes de éstas»*.

4.4 Versión definitiva

Sobre esta versión, realizada el 10 de septiembre de 2007, se emiten una Memoria justificativa del proyecto y una memoria económica. En relación a la Memoria justificativa, la misma desgrana algunos de los puntos ya analizados con anterioridad y relativos a la necesidad de un nuevo reglamento.

Por su parte, la Memoria económica, destaca que, desde la perspectiva de valoración de costes, la novedad esencial aportada por el Reglamento consiste en la extensión de la aplicación de las medidas de seguridad a los ficheros y tratamientos no automatizados de datos de carácter personal, frente al régimen establecido por el Reglamento de Medidas de Seguridad que los limitaba a los tratamientos automatizados.

Desde esta perspectiva, se analiza el impacto económico en una y otra clase de ficheros, basándose las valoraciones en una muestra de 893.568 ficheros, correspondientes a los ficheros inscritos en el Registro General de Protección de Datos a 21 de mayo de 2007. La memoria entiende que la reglamentación proyectada sólo supondrá un incremento de gasto para los ficheros automatizados a los que se imponga un nivel de seguridad mayor que el previsto en Reglamento de Medidas de Seguridad. Para los ficheros no automatizados se realiza una estimación diferenciando las medidas de seguridad en técnicas y organizativas.

201 Tribunal Constitucional, Pleno, Sentencia 228/2003 de 18 de diciembre de 2003, Recurso 3342/1995

La memoria concluye considerando que la disposición proyectada no implica incremento de gasto ni disminución de ingreso para la Hacienda Pública estatal. Finalmente, el expediente, fue remitido al Consejo de Estado para la emisión de dictamen y aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre.

5. Después del Reglamento

Con la finalidad de garantizar la seguridad jurídica el legislador, en la aprobación de la Ley Orgánica de Protección de Datos, declaró subsistentes las normas reglamentarias existentes a la fecha:

- • Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Con carácter complementario, se habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.

Mediante el Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007 se ha cumplido con esta habilitación poniendo fin al régimen de subsistencia de los reglamentos de desarrollo de la LORTAD y fijando el marco normativo de aplicación que actualmente aparece configurado de forma principal por la Ley Orgánica 15/1999 y su reglamento de desarrollo.

Por tanto, ha quedado derogadas las siguientes normas, tal y como establece la Disposición Derogatoria Única del Reglamento de Desarrollo de la LOPD:

- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los

datos de carácter personal.

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el Reglamento de Desarrollo de la LOPD.

6 El Reglamento de desarrollo de la LOPD

El Reglamento se ha elaborado con la intención de no duplicar o reiterar los contenidos en la Ley Orgánica de Protección de Datos así como de dotar de un desarrollo reglamentario específico a la Ley Orgánica, tal y como dispone en su primer artículo, que hace referencia además, a otras dos normas respecto a las cuales también se lleva a cabo el necesario desarrollo reglamentario con respecto al desarrollo de las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora:

- Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico.
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

6.1 Estructura

La norma se estructura en el primero de los cuales contiene los artículos dedicados a delimitar su objeto y ámbito de aplicación. El Título II, desarrolla los principios de la protección de datos del cual es destacable la regulación del modo de captación del consentimiento o la forma en la que se articula la figura del encargado de tratamiento. El título III se ocupa de los derechos de las personas con respecto a sus datos personales. Por su parte, el título IV viene a clarificar aspectos importantes de interpretación de la LOPD en puntos concretos, detallando las pautas a seguir respecto de los ficheros que recogen datos sobre solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial. El título V es el primero de los dedicados a las obligaciones materiales y formales que atañen a los responsables de ficheros, describiendo las fases de creación, notificación e inscripción de ficheros de titularidad pública y privada. Las obligaciones asociadas a las transferencias internacionales de datos, ocupan el título VI y una regulación detallada de la figura de los Códigos Tipo, el título VII. Pero es el título VIII el más importante de los dedicados a

las obligaciones de los responsables, ya que regula las medidas de seguridad en el tratamiento de datos de carácter personal. Por último, el título IX se dedica a los procedimientos tramitados por la Agencia Española de Protección de Datos, título en el que se ha optado por regular exclusivamente las especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al Reglamento.

6.2 Entrada en vigor del Reglamento de desarrollo de la LOPD

Los plazos de aplicación del Reglamento de desarrollo de la LOPD han sido establecidos por las Disposiciones Transitorias del Real Decreto 1720/2007:

- **Entrada en vigor:** La fecha general para la entrada en vigor del Reglamento se estableció mediante la aplicación de un plazo de tres meses desde su publicación, por lo que el Reglamento de desarrollo de la LOPD está en vigor desde el 20 de abril de 2008.
- **Adaptación de los Códigos Tipo:** En el plazo de un año desde la entrada en vigor del Reglamento de desarrollo de la LOPD, se deberán notificar a la Agencia Española de Protección de Datos las modificaciones en los Códigos Tipo, es decir, desde el : 20 de abril de 2009.
- **Implantación de las medidas de seguridad:** Se han establecido distintos plazos en función del tipo de ficheros y del nivel de los datos:
  - Ficheros Automatizados:
    - **Regla general:** Un año desde la entrada en vigor, es decir, desde el 20 de abril de 2009.
    - **Excepciones:** Dieciocho meses para la aplicación de las medidas a:
      - Ficheros que contengan datos derivados de actos de violencia de género.
      - Datos de tráfico y localización en ficheros de operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas.
  - Ficheros no automatizados :
    - Ficheros de nivel básico: Un año, es decir, desde el 20 de abril de 2009.
    - Nivel medio: Dieciocho meses, es decir, desde el 20 de octubre de 2009.
    - Nivel alto: Dos años, es decir, desde el: 20 de abril de 2010.

Por último, la Disposición Transitoria Segunda dispone a este respecto en su punto tercero:

«*3. Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente Real Decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo*».

Por lo tanto, debemos tener en cuenta que todos los ficheros que contengan datos personales creados con posterioridad al 20 de abril de 2008, deberán haber implantado todas las medidas exigidas por el Reglamento de desarrollo de la LOPD.

- **Ejercicio de derechos y otros procedimientos:** El Reglamento de desarrollo de la LOPD cierra sus previsiones para la entrada en vigor de la norma con sus disposiciones transitorias tercera, cuarta y quinta, en las que se ocupa de la entrada en vigor de las nuevas disposiciones relativas al ejercicio de derechos, procedimientos y actuaciones previas que pudieran haber sido efectuadas antes del 20 de abril de 2008. Como no podía ser de otra forma, todos estos procedimientos se seguirán rigiendo por la normativa anterior, en vigor cuando se iniciaron.

II. Novedades en el Reglamento de Desarrollo

Una vez analizados los antecedentes y estructura del Reglamento de Desarrollo de la LOPD y puesta la norma en el contexto que llevó a su promulgación y en relación con el resto de la normativa aplicable, corresponde ahora, centrarse en el análisis de las principales novedades incorporadas en su texto. Por tanto, vamos a analizar las principales novedades aportadas por una norma que tiene como misión principal, solucionar los problemas detectados en la Ley Orgánica de Protección de Datos a lo largo de sus casi diez años de aplicación.

1 Ámbito objetivo de aplicación

El ámbito objetivo de aplicación de la norma ha sido definido en el artículo 2 Reglamento de desarrollo de la LOPD que, en desarrollo del artículo 2 de la Ley Orgánica de Protección de Datos establece:

*«**Artículo 2. Ámbito objetivo de aplicación.***
1. El presente Reglamento 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.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. 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.»

Quizá lo más llamativo del presente artículo es la regla general establecida en su primer punto, que recoge literalmente el contenido del artículo 2 de la Ley Orgánica y, conforme al que el ámbito objetivo de aplicación se refiere a la existencia de datos de carácter personal *«susceptibles de tratamiento»*. Sin duda, hubiera sido preferible una mayor concreción -o si se prefiere un alineamiento con lo establecido tanto por la Directiva 95/46/CE como por la propia Ley Orgánica de Protección de Datos- en el sentido de resaltar que, en todo caso, el objeto de la regulación no son directamente los datos personales, sino el hecho de que éstos sean objeto de tratamiento.

Pero no todo han de ser críticas, la parte acertada de este artículo es que el Reglamento de desarrollo de la LOPD es aplicable a los datos personales objeto de tratamiento no automatizado. Asimismo es remarcable como el artículo 2 del Reglamento de desarrollo de la LOPD entra a regular determinados aspectos respecto a los que la aplicación práctica de la LOPD había puesto de manifiesto la necesidad de una regulación más detallada y sobre los que vamos a puntualizar a continuación.

1.1 Datos de personas fallecidas

Tal y como establece el artículo 2.4 del Reglamento de desarrollo de la LOPD, se establecen algunas consideraciones respecto a los datos de personas fallecidas que debemos tener en cuenta. En primer lugar, se establece una regla general de exclusión de estos tratamientos. Se trata de un tema que a lo largo de los años de vigencia de la LOPD ha sido tema de debate no más de una vez. En efecto, la aplicabilidad del régimen jurídico establecido en la Ley Orgánica de Protección de Datos ha sido objeto de análisis en distintos informes y resoluciones de la Agencia, siempre en el sentido expresado por esta regla general de exclusión: El régimen jurídico de aplicación a los datos de carácter personal no será de aplicación a los datos de personas fallecidas.

En este sentido podemos citar un Informe de la Agencia Española de Protección de Datos[202] que señala:

«La consulta plantea dudas sobre la posibilidad de comunicar datos de personas fallecidas y su

202 Agencia Española de Protección de Datos (2006). Informe 365/2006: *«Tratamiento y cesión de datos de personas fallecidas»* [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2006-0365_Tratamiento-y-cesi-oo-n-de-datos-de-personas-fallecidas.pdf

adecuación a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal. (…)

La resolución de la cuestión planteada deberá obtenerse en función de la naturaleza misma del derecho protegido por la norma, lo que conduce a la necesidad de determinar si la muerte de las personas da lugar a la extinción del derecho a la protección de la "privacidad" o a la denominada "libertad informática", regulada por la Ley Orgánica 15/1999, ya que el artículo 32 del Código Civil dispone que "la personalidad civil se extingue por la muerte de las personas", lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

Como cuestión previa, es necesario indicar que esta Agencia de Protección de Datos ha venido tradicionalmente poniendo de manifiesto que el derecho fundamental a la protección de datos es un derecho personalísimo que, en consecuencia, se extingue por la muerte de las personas.

Este razonamiento ha venido amparándose en la vinculación existente entre el derecho a la protección de datos y la intimidad de las personas, si bien debe seguir considerándose aplicable tras la configuración otorgada a la protección de datos como derecho fundamental de la persona por la Sentencia 292/2000, de 30 de noviembre del Tribunal Constitucional.

(…)

No obstante, debe recordarse que si bien el derecho a la protección de datos desaparecería como consecuencia de la muerte de las personas, no sucede así con el derecho de determinadas personas para ejercitar acciones en nombre de las personas fallecidas, con el fin de garantizar otros derechos constitucionalmente reconocidos. Así, por ejemplo, cabe destacar que la Ley Orgánica 1/1885, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pone de manifiesto en sus artículos 4 a 6 que el fallecimiento no impide que por las personas que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya designado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal.

Por este motivo, los supuestos a los que se refiere la consulta no se encontrarían, en principio, sometidos al régimen previsto en la Ley Orgánica 15/1999, al referirse exclusivamente a personas fallecidas y en consecuencia desde el punto de vista de la normativa sobre protección de datos

personales, no existe inconveniente a las comunicaciones de datos planteadas.

No obstante, si bien los supuestos descritos en la consulta no se encontrarían, en principio, sometidos al régimen previsto en la Ley Orgánica 15/1999, al referirse exclusivamente a personas fallecidas, sí será preciso que por la entidad que trata los datos se adopten medidas que impidan el conocimiento por terceros a otro tipo de datos de los fallecidos, toda vez que dicho conocimiento pudiera dar lugar al ejercicio de acciones por las personas legalmente habilitadas en defensa de otros bienes jurídicamente protegidos que no se extinguen como consecuencia de la muerte de las persona».

Una vez fijada esta regla general, el artículo 2.4 Reglamento de desarrollo de la LOPD matiza, en el supuesto de personas vinculadas al fallecido, la posibilidad de que las mismas comuniquen la defunción del titular de los datos e insten la cancelación de sus datos.

Respecto a esta excepción, la Agencia Española de Protección de Datos, en su Informe al Borrador del Reglamento, declaró:

«Parece conveniente que el Reglamento prevea una cautela para garantizar que, habiéndose producido el fallecimiento del afectado, será como regla general de aplicación lo dispuesto en el artículo 4.5 de la Ley Orgánica 15/1999, a cuyo tenor los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, de forma que serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados».

Sin embargo, no dejan de plantearse dudas sobre en qué casos se puede estimar que existe una *vinculación suficiente* con el fallecido así como si deberán cancelarse todos los datos personales del fallecido en el caso de que lo requiera una de las personas vinculadas. En línea con lo establecido por el Dictamen del Consejo de Estado al Proyecto de Reglamento, el Reglamento de desarrollo de la LOPD incluye los siguientes requisitos al respecto:

- En primer lugar, el Consejo de Estado estableció la necesidad de incluir alguna aclaración adicional al concepto de *"persona vinculada"* al objeto de poder identificar adecuadamente la legitimación de estos solicitantes. En este sentido se incluyó la referencia *"por razones familiares o análogas"*. Por lo tanto, cabe concluir que el ejercicio de la potestad prevista en

el artículo 2.4 del Reglamento de desarrollo de la LOPD, se reserva a aquellas personas que guarden con el afectado una relación familiar o bien una relación afectiva similar -parejas de hecho-.

- En segundo lugar, hay que concluir que no en todos los casos cabe la cancelación de los datos personales del fallecido. Así, la Agencia Española de Protección de Datos, en su Dictamen, señalaba el supuesto de los tratamientos que se limitan a reproducir la realidad de una determinada situación de hecho, como por ejemplo los datos de bautismo que constan en los registros de la Iglesia Católica. Por esta razón , el artículo 2.4 del Reglamento de desarrollo de la LOPD incluye la mención *"y solicitar, cuando hubiere lugar a ello, la cancelación de los datos"*.

1.2 Empresarios individuales

El artículo 2.3 del Reglamento de desarrollo de la LOPD, es uno de los preceptos cuya redacción fue más controvertida a lo largo de la tramitación del Reglamento. Podemos sintetizar la doctrina de la Agencia Española de Protección de Datos a este respecto en las siguientes líneas[203]:

«Conviene recordar que de los artículos 1 y 2.1 de la LOPD se deduce claramente que el ámbito subjetivo de aplicación de la LOPD no ampara a las personas jurídicas, y que, tan sólo, resulta aplicable al tratamiento de datos de carácter personal relacionados con personas físicas.

El fundamento de la delimitación de este ámbito de aplicación reside en que si la protección de los datos personales se refiere a la intimidad personal y familiar, no puede entenderse que las empresas gocen de la citada intimidad y, por tanto, no puede ser aplicable a éstas, aún cuando la actividad de la empresa en el tráfico jurídico se deba realizar, necesariamente, a través de un apoderamiento a favor de una persona física.

De este modo, quedarán excluidos de las garantías de la LOPD los datos que se refieran a personas jurídicas, en todos los casos, así como a los profesionales (en aquellos casos en los que organicen su actividad bajo la forma de empresa, ostentando, en consecuencia, la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y a los empresarios individuales siempre que su actividad comercial o profesional pueda diferenciarse en

203 Agencia Española de Protección de Datos (2007). Resolución de 27 de julio de 2007 [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/TD-00266-2007-en.pdf

cada caso, de manera clara y determinante, de su propio entorno de privacidad como persona física».

Esta interpretación se hace eco de distintas resoluciones anteriores así como del criterio fijado por la Audiencia Nacional, que diferencia a los empresarios individuales de los profesionales que no hayan organizado su actividad en forma de empresa.

Por otra parte, este criterio que quizá no ha sido convenientemente matizado en Reglamento de desarrollo de la LOPD, obliga a analizar caso por caso si los datos aparecen exclusivamente vinculados a la actividad mercantil del empresario o si confluyen la esfera mercantil y profesional del comerciante, en cuyo caso debemos entender que se aplica la Ley Orgánica de Protección de Datos y su normativa de desarrollo.

En este sentido cabría establecer las siguientes pautas:

- El reglamento será aplicable a los tratamientos de datos relativos a empresarios individuales cuando no sea posible diferenciar su actividad mercantil de su propia actividad privada.
- El reglamento será aplicable a los tratamientos de datos relativos a profesionales cuando estos no tengan organizada su actividad profesional en forma de empresa.

1.3 Contactos profesionales

El artículo 2.2 del Reglamento, se refiere a los datos de las personas de contacto en las empresas. De acuerdo a lo establecido por dicho artículo el Reglamento no será aplicable a los tratamientos de datos de personas jurídicas ni a aquellos que se limiten a incorporar datos de personas físicas que presten sus servicios en aquellas.

El precepto recoge la interpretación que la Agencia Española de Protección de Datos ha venido realizando a lo largo de estos años, y conforme a la cual en los casos en los que la recogida de datos se limite a las actuaciones de personas físicas en relación de personas jurídicas, debe entenderse que dicho tratamiento se encuentra fuera del ámbito objetivo de la norma[204]:

«(...) ambos interlocutores intervienen en el presente supuesto, como ha quedado acreditado, en el

204 Agencia Española de Protección de Datos (2005). Resolución de 19 de julio de 2005.

desempeño de las funciones de apoderamiento que le son propias como representantes de las citadas entidades, desarrollando, en todo momento, una actividad mercantil claramente separada de sus respectivas actividades privadas.

(...) los hechos expuestos se circunscriben a unas actuaciones desarrolladas, por los representantes de las sociedades implicadas, exclusivamente en el ámbito de actuación de las mismas, y en concreto en el desarrollo de la actividad inmobiliaria que constituye su objeto social, que, como ha quedado señalado, comprende la construcción, promoción, adquisición y venta de inmuebles. En consecuencia, el tratamiento de los datos de que traen causa las presentes actuaciones de inspección no se encuentra incluido dentro del ámbito de aplicación establecido en la LOPD».

Para poder establecer que el tratamiento de los datos de una persona física es accesorio a la finalidad perseguida, deben concurrir dos requisitos:

- Los datos tratados deberán limitarse a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios. De acuerdo con esto, el Reglamento de desarrollo de la LOPD impone que el tratamiento se limite a los datos de nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales. Por lo tanto, cualquier otro dato adicional, no sería necesario para el mantenimiento del contacto empresarial.
- Asimismo es necesario tener en cuenta la finalidad que justifica el tratamiento. En relación con dicha finalidad, la Agencia Española de Protección de Datos ha establecido[205]: «*La inclusión de los datos de la persona de contacto debe ser meramente accidental o incidental respecto de la verdadera finalidad perseguida por el tratamiento, que ha de residenciarse no en el sujeto, sino en la entidad en la que el mismo desarrolla su actividad o a la que aquél representa en sus relaciones con quienes tratan los datos.*
  De este modo, la finalidad del tratamiento debe perseguir una relación directa entre quienes traten el dato y la entidad y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esa finalidad.
  Así sucedería en caso de que el tratamiento responda a relaciones "business to business", de modo que las comunicaciones dirigidas a la empresa, simplemente, incorporen el nombre

205 Agencia Española de Protección de Datos (2008). Informe 0156/2008: Medidas de seguridad en los ficheros de nóminas y demás especialidades [en línea]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/reglamento_lopd/common/pdfs/2008-0156_Medidas-de-seguridad-en-los-ficheros-de-n-oo-minas-y-dem-aa-s-especialidades.pdf

de la persona como medio de representar gráficamente el destinatario de la misma. Por el contrario, sin la relación fuera "business to consumer", siendo relevante el sujeto cuyo dato ha sido tratado no sólo en cuanto a la posición ocupada sino como destinatario real de la comunicación, el tratamiento se encontraría plenamente sometido a la Ley Orgánica 15/1999, no siendo de aplicación lo dispuesto en el artículo 2.2 del Reglamento».

2. Principios

El Título II del Reglamento de desarrollo de la LOPD desarrolla los principios de la protección de datos establecidos por la Ley Orgánica. Nos encontramos en presencia de un Título de vital importancia, en tanto en cuanto, la naturaleza de estos principios constituyen la base sobre la que se sustenta la protección de datos de carácter personal. En este sentido y si bien, todos los principios de la materia que nos ocupa, son importantes, interesa prestar especial atención al principio de calidad de los datos, al deber de información al interesado o afectado y al principio de consentimiento.

2.1 Calidad de los datos

Se encuentra regulado en los artículos 8 al 11 del Reglamento de desarrollo de la LOPD y desarrolla el principio de calidad de acuerdo a lo establecido por la Ley Orgánica de Protección de Datos.

El artículo 8, que lleva por título *«Principios relativos a la calidad de los datos»*, es bastante extenso y se fundamenta no solo en el artículo 4 de la Ley Orgánica de Protección de Datos, sino también en los principios de consentimiento, información, calidad, finalidad, seguridad, proporcionalidad y legalidad de los tratamientos.

En este sentido, el artículo 8.1 establece que los tratamientos realizados sean en todo caso legítimos y leales mientras que, por su parte, el 8.2, el 8.3 y el 8.4 se centran en el cumplimiento de la finalidad para la cual se obtuvieron los datos de carácter personal.

Sin embargo, interesa destacar el artículo 8.5 ya que en él se establecen las principales novedades articuladas por el Reglamento de Desarrollo de la LOPD:

- Se recoge una presunción, sobre la que se admite prueba en contra, que libera al responsable del tratamiento de velar por la exactitud de los datos cuando estos los hubiera facilitado directamente el afectado, ya que «*si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste*».
- Se establece un plazo de 10 días para la cancelación de oficio por parte del responsable de tratamiento, de los datos inexactos o incompletos. La presente actualización deberá llevarse a cabo sin que el titular lo solicite recayendo directamente la obligación sobre el responsable del tratamiento.
- Corresponde al responsable comunicar los datos rectificados a aquellos terceros a los que les hayan sido cedidos con la finalidad de que estos procedan a su vez a actualizarlos, otorgándose un plazo de 10 días para comunicar y otros 10 días más para que el cesionario proceda a actualizar la información.

2.2 Consentimiento

En todo aquello relativo al principio de consentimiento para el tratamiento de datos de carácter personal, el Reglamento de desarrollo de la LOPD significa un gran avance. Los artículos 10 a 17 de la citada norma versan sobre la forma de prestación del consentimiento.

En dichos artículos se recogen aspectos esenciales que completan a la Ley Orgánica de Protección de Datos de Carácter Personal.

De esta forma, el artículo 10 Reglamento de desarrollo de la LOPD, regula los supuestos que legitiman el tratamiento o la cesión de datos personales desarrollando puntos ya recogidos en la LOPD. Asimismo se incluyen algunas novedades como la posibilidad de proceder al tratamiento de datos personales sin consentimiento del interesado cuando dicho tratamiento tenga por objeto la satisfacción de un interés legítimo del responsable del fichero. Previsión que si bien no era recogida por la Ley Orgánica de Protección de Datos de Carácter Personal, si se encuentra recogida en la Directiva 95/46/CE.

En este sentido los responsables del tratamiento, cuando capten datos de carácter personal deberán tener en cuenta lo siguiente:

- Es necesario recabar un *"consentimiento inequívoco"* tal y como se establece en el artículo

6 de la Ley Orgánica de Protección de Datos, teniendo en cuenta lo estipulado en el artículo 12.1 del Reglamento de desarrollo de la LOPD, que exige que la solicitud de consentimiento *"deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como las restantes condiciones que concurran"*. Esto supone que será nulo el consentimiento requerido para la cesión de datos personales cuando no se haya informado inequívocamente, al interesado o afectado, sobre la finalidad del tratamiento y sobre la actividad del cesionario y que se sitúa en consonancia con la interpretación mantenida por la Agencia Española de Protección de Datos en este sentido y que no es otra que considerar que el consentimiento inequívoco no puede equipararse con el consentimiento expreso y que cabe el consentimiento tácito.

- Es posible tratar datos personales de menores de edad si bien:
  - Los mayores de catorce años pueden prestar su consentimiento en aquellos casos en los que la Ley no exija para su prestación la asistencia de los titulares de la patria potestad siendo necesario, en estos casos, que el responsable del fichero establezca procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor así como la autenticidad del consentimiento prestado por este o por sus representantes legales.
  - No podrán recabarse datos de menores de edad que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección de los padres o tutores con la única finalidad de recabar la autorización citada anteriormente.
- El Reglamento de desarrollo de la LOPD articula procedimiento para recabar el consentimiento aplicable excepto en los casos en los que la Ley Orgánica exige el consentimiento expreso. Sobre este punto han de tenerse en cuenta las siguientes consideraciones:
- El responsable se dirigirá al afectado, informándole de acuerdo a los requerimientos legales y ofreciéndole un plazo de 30 días para manifestar su negativa.
- Debe habilitarse un medio sencillo y gratuito para ello.
- No será posible reiterar la solicitud a través de este mismo procedimiento en el plazo de un año.
- Deberán establecerse todos aquellos protocolos necesarios para garantizar la capacidad del responsable del tratamiento, de acreditar la prestación de dicho consentimiento.
- Cuando se solicite el consentimiento en el marco de un contrato, para fines distintos a los recogidos en el mismo, deberá permitirse al afectado que manifieste su negativa en el

mismo, mediante una casilla visible y no marcada con anterioridad.

- El consentimiento podrá ser revocado, estando obligado, el responsable del tratamiento, a habilitar un medio sencillo y gratuito así como de cesar en el tratamiento en el plazo de 10 días.

2.3 Deber de información

Si bien es cierto que el Reglamento de desarrollo a articulado pocas modificaciones en el deber de información, no es menos cierto que deben ser mencionadas:

- El responsable de tratamiento debe ser capaz de acreditar el cumplimiento de la obligación de información al interesado contenida en el artículo 5 de la Ley Orgánica de Protección de Datos. Por esta razón, el artículo 18 Reglamento de desarrollo de la LOPD, le impone la obligación de conservar los soportes utilizados para informar. Se trata de una nueva obligación cuya aplicación plantea numerosas interrogantes a pesar de que el propio Reglamento prevé que la conservación pueda hacerse en soportes digitales, admitiéndose el escaneado del papel, siempre y cuando se garantice que el proceso de digitalización no ha alterado el original. Asimismo y, en supuestos de condiciones normales -en el caso de consentimientos expresos-, podrá conservarse el documento firmado, la grabación de la conversación telefónica o los registros de la navegación por Internet. Para los supuestos de consentimiento tácito, esta prueba es mucho más compleja, siendo necesario establecer los medios para probar -aunque sea de manera indiciaria-, que el consentimiento se ha prestado.
- Se aclaran los supuestos de operaciones de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial así como de cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la legislación mercantil. Dichas situaciones, en ningún caso, supondrán una cesión o comunicación de datos sin que esto signifique que el responsable del fichero o tratamiento no deba de cumplir con el pertinente deber de información, para con el interesado o afectado, establecido en el artículo 5 de la Ley Orgánica de Protección de Datos.

3. El encargado del tratamiento

El capítulo III del Título II del Reglamento de desarrollo de la LOPD regula la figura del Encargado de Tratamiento, establecida por el artículo 12 de la Ley Orgánica.

Siguiendo a Piñar Mañas[206], se trata de la regulación más completa que hasta el momento se ha producido de tal figura, hasta el punto de que la Exposición de Motivos del Real Decreto 1720/2007 afirma, quizás de forma algo grandilocuente, que ofrece *«lo que no puede definirse sino como un estatuto del encargado de tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura»*.

Las principales novedades en esta figura se encuentran en todo lo relativo a la subcontratación así como en todo lo relativo a la conservación de los datos por parte del responsable del tratamiento.

3.1 Subcontratación

Si bien se trata de una novedad establecida por el Reglamento de desarrollo de la LOPD, no podemos obviar el importante precedente que, en materia de subcontratación, supuso la aprobación de la Ley 30/2007, de Contratos del Sector Público, que en su Disposición Adicional Trigésimo Primera, relativa a los datos de carácter personal, establecía ya la posibilidad de subcontratar estableciendo una serie de garantías a cumplir.

3.1.1 Subcontratación en nombre y por cuenta del responsable

Tal y como establece el artículo 21.1 del Reglamento de desarrollo de la LOPD:

«El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento».

206 PIÑAR MAÑAS, J. (2008): *«Novedades en relación con la figura del Encargado del Tratamiento»* en *«Protección de Datos. Comentarios al Reglamento»*. Editorial Lex Nova. Valladolid. Página 217.

De la lectura de este artículo casi podríamos decir que no existe una verdadera subcontratación, ya que el encargado actúa en nombre y por cuenta del responsable. No obstante y, dejando al margen esta polémica, deberán cumplirse los siguientes requisitos:

- La autorización debe ser previa y expresa.
- La autorización deberá poder acreditarse y por tanto, no se presume.
- El contrato que, a nombre del responsable, se celebre entre las partes, deberá cumplir con las garantías articuladas por el artículo 12 de la Ley Orgánica de Protección de Datos.

3.1.2 Subcontratación de servicios sin necesidad de autorización previa

Tal y como establece el artículo 21.2 del Reglamento de desarrollo de la LOPD, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan determinados requisitos:

- Que se especifiquen en el contrato los servicios que se puedan contratar y, si fuera posible, la empresa con la que se vaya a subcontratar.
- Que el tratamiento de datos por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
- Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato en los términos previstos en la normativa sobre protección de datos de carácter personal.

3.1.3 Subcontratación sobrevenida, necesaria y no prevista en el contrato

El artículo 21.3 del Reglamento de desarrollo de la LOPD prevé la posibilidad de que durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato.

Siguiendo el análisis de Piñar Mañas[207], distinguimos los siguientes requisitos para este tipo de subcontratación:

- • La subcontratación ha de ser necesaria, no simplemente conveniente u oportuna. Por el

207 PIÑAR MAÑAS, J. (2008): *«Novedades en relación con la figura del Encargado del Tratamiento»* en *«Protección de Datos. Comentarios al Reglamento»*. Editorial Lex Nova. Valladolid. Página 244.

carácter necesario de la misma es por lo que el Reglamento permite que, pese a no estar previsto en el contrato, pueda subcontratarse una parte de los servicios.

- La subcontratación sólo es posible en relación con una parte de las prestaciones, no con la totalidad.
- Deberán someterse al responsable del tratamiento los extremos señalados en el artículo 21.1 Reglamento de desarrollo de la LOPD.

3.2 Conservación de los datos por el encargado de tratamiento

El artículo 22.1 del Reglamento de desarrollo de la LOPD contiene la regla general establecida por el artículo 12.3 de la Ley Orgánica de Protección de Datos:

«Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento».

En este sentido, la principal novedad radica en el reconocimiento de la posibilidad de que el responsable del tratamiento designe a un encargado de recibir los datos.

Hablamos de un supuesto de aplicación en caso de que una vez cumplida la prestación contractual, el responsable del fichero entable una nueva relación contractual con un encargado diferente del anterior. En este caso, el Reglamento de desarrollo de la LOPD admite que los datos sean entregados directamente al nuevo encargado designado por el responsable. No obstante, para la realización de esta entrega se recomienda:

- Acreditar que el encargado actúa en nombre del responsable. Para ello puede suscribirse entre ambos un documento especificando los datos de identificación del nuevo encargado.
- Suscribir el correspondiente contrato con el nuevo encargado, en los términos del artículo 12 de la Ley Orgánica de Protección de Datos.

Asimismo, el artículo 22 del Reglamento de desarrollo de la LOPD prevé dos supuestos relativos a la destrucción de los datos así como respecto de su bloqueo que también presentan novedades:

- No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
- Se establece la obligación de que el encargado conserve, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades en su relación con el responsable de tratamiento[208].

4. Ejercicio de derechos

El Título III, del Reglamento de desarrollo de la LOPD, regula los derechos de acceso, rectificación, cancelación y oposición, que a su vez y como ya tuvimos oportunidad de ver con anterioridad, se regulan en los artículos 15 a 18 de la Ley Orgánica de Protección de Datos.

De forma previa ya habían sido enunciados por la LORTAD, y fueron objeto de desarrollo en el Real Decreto 1332/1994, de 20 de junio[209], norma que la Ley Orgánica de Protección de Datos mantuvo vigente en todo lo que no se opusiera a su contenido y que finalmente ha sido derogada por la Disposición Derogatoria Única del Real Decreto 1720/2007.

Asimismo, en esta materia, debe tenerse en cuenta la Instrucción 1/1998 de la Agencia Española de Protección de Datos[210], que ha completado durante estos años la regulación del ejercicio de los derechos de los interesados y que ha servido como base para la regulación establecida en el Reglamento de desarrollo de la LOPD.

208 Nótese que el Reglamento de desarrollo de la LOPD establece por tanto un nuevo deber para el encargado de tratamiento: el de conservar bloqueados los datos durante un plazo que puede llegar a ser mayor que el fijado en el contrato.

209 Ministerio de Justicia e Interior. Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Publicado en el Boletín Oficial del Estado n.º 147 de 21 de junio de 1994 [en línea]. Disponible en: http://www.boe.es/boe/dias/1994/06/21/pdfs/A19199-19203.pdf

210 Agencia Española de Protección de Datos (1998). «*Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.*» [en línea]. Disponible en: http://noticias.juridicas.com/base_datos/Admin/i1-1998-apd.html [2011, 7 de julio]

En base a todos estos antecedentes, el Reglamento de desarrollo de la LOPD ha venido a completar la regulación aplicable, incluyendo aspectos novedosos que deben contribuir garantizar el ejercicio de los derechos así como estableciendo algunas obligaciones para los responsables de los ficheros:

- **Obligaciones generales**
  - Para el ejercicio de derechos, se prevé una forma adicional de representación que permita ejercitarlos a través de representante voluntario, expresamente designado. En ese caso se exige que conste claramente acreditada la identidad del representado así como la representación conferida por aquél.
  - Se incluye la obligación de ofrecer al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Dicho ejercicio nunca podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan, no considerándose conforme la obligación de envío de cartas certificadas, utilización de servicios telefónicos de tarificación adicional o medios análogos.
  - El responsable del fichero deberá atender la solicitud aún cuando el interesado mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos mínimos requeridos.
  - En cuanto al procedimiento, el artículo 25.1 a) del Reglamento de desarrollo de la LOPD, incorpora nuevas vías admitiendo la utilización de medios electrónicos para la acreditación de la identidad del interesado e indicando expresamente que la utilización de la firma electrónica identificativa del afectado eximirá de la presentación del Documento Nacional de Identidad.
  - Se establece una obligación para el responsable del tratamiento, que si bien ya se deducía de la regulación anterior, se añade ahora de forma expresa: la obligación de conservar la acreditación del cumplimiento de los deberes relacionados con el ejercicio de los derechos: *«corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta»*.
  - Se prevé el caso especial del ejercicio de derechos ante un encargado de tratamiento. Se recoge la obligación del encargado de dar traslado de la solicitud al responsable a fin de que el mismo lo resuelva salvo que en la relación regulada por contrato entre ambos, se prevea expresamente que el encargado atenderá dichas solicitudes.

- **Derecho de acceso**
  - Si existen razones de complejidad que lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros concretos a los que desee acceder o podrá restringir los sistemas de consulta en función de la configuración o la implantación material del fichero.
  - El responsable del tratamiento está obligado a cumplir con las medidas de seguridad, pero, en el caso de que el interesado rechazase las vías de acceso establecidas, se exime a aquel de la responsabilidad que pudiera derivarse de los riesgos que para la información pudieran tener.
  - Se incluye la obligación para el responsable del fichero de, en caso de denegación de acceso, informar al afectado sobre la posibilidad de recabar la tutela de la Agencia Española de Protección de Datos o de su homólogo autonómico. Esta obligación se incluye también para la denegación de los derechos de rectificación y cancelación.

- **Derechos de rectificación y cancelación**
  - Se extiende el plazo concedido al responsable del tratamiento para resolver sobre la solicitud de rectificación o cancelación que pasa de 5 a 10 días a contar desde la recepción de la solicitud. Este plazo también se aplica al cesionario para llevar a cabo la solicitud del interesado.
  - La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos establecidos por la Ley Orgánica de Protección de Datos.

- **Derecho de oposición**
  - Se define como el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:
    - Cuando no sea necesario su consentimiento para el tratamiento. En este caso, deberán alegarse motivos fundados y legítimos para su ejercicio.
    - Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
    - Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y se base, de forma exclusiva, en un tratamiento automatizado de sus datos de carácter personal
  - Se establece un plazo de 10 días para resolver sobre la petición, a contar desde la

recepción de la solicitud.

5. Medidas de seguridad

5.1 Aplicación de niveles de seguridad

La primera novedad fundamental viene referida a la aplicación de los niveles de seguridad.

El artículo 81 del Reglamento de desarrollo de la LOPD determina las reglas a seguir en este caso en función de la naturaleza de los datos personales gestionados.

5.1.1 Ficheros de nivel medio (calificación)

A lo ya establecido por el ya derogado Reglamento de Medidas de Seguridad, el Reglamento de desarrollo de la LOPD añade:

«Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social».

Asimismo, el artículo 81 Reglamento de desarrollo de la LOPD determina, de forma más precisa, otro de los supuestos de implantación de medidas de seguridad de nivel medio:

«Serán de aplicación estas medidas de seguridad en los casos en los que los ficheros "contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos"».

5.1.2 Ficheros de nivel alto (calificación)

Se incluyen, entre los datos a los que serán de aplicación medidas de nivel alto:

- Ficheros que contengan datos derivados de actos de violencia de género.
- Se incluyen expresamente los datos de afiliación sindical, categoría que si bien ya estaba incluida implícitamente como dato de nivel alto en el antiguo reglamento de medidas de seguridad, no se mencionaba de forma expresa.

No obstante, tanto respecto a estos datos de afiliación sindical como a los de ideología, religión, creencias, origen racial, salud o vida sexual, el Reglamento de desarrollo de la LOPD prevé que puedan adoptarse las medidas de nivel básico en los siguientes casos:

- Cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- Cuando nos encontremos en presencia de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
- Para los datos relativos a la salud, cuando se trate de datos referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
- En el caso de los ficheros responsabilidad de operadores que prestan servicios de comunicaciones electrónicas disponibles al público o que exploten redes públicas respecto a los datos de tráfico y a los datos de localización, se añade la obligación de implantar el registro de acceso, establecido en el artículo 103 del Reglamento de desarrollo de la LOPD.

5.2 Medidas aplicables a todos los ficheros que contengan datos personales

La regulación de las medidas de seguridad aplicables a los ficheros no automatizados, ha implicado que el articulado del Reglamento de desarrollo de la LOPD recoja, en primer lugar, las medidas aplicables a todos los ficheros, y que posteriormente, se detallen las aplicables a los automatizados y a los no automatizados.

Es por lo tanto de aplicación general lo dispuesto en relación al Documento de Seguridad, que de acuerdo con el Reglamento de desarrollo de la LOPD, deberá contener, necesariamente una serie de puntos en los que se identifican las siguientes novedades:

- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.
- Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.
- Se deberá designar uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar en el documento de seguridad.
- Cuando los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica de Protección de Datos, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

5.3 Ficheros automatizados

5.3.1 Medidas para todos los tratamientos

El Reglamento de desarrollo de la LOPD ha establecido la obligación de implantar medidas que antes se reservaban a los ficheros de nivel medio a todos los ficheros automatizados:

- Cuando los datos se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero será necesario que exista una autorización previa del responsable del fichero y deberá en todo caso garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. Esta autorización tendrá que constar en el documento de seguridad.
- La salida de soportes y documentos que contengan datos de carácter personal fuera de los locales bajo el control del responsable del fichero deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad. Se incluye expresamente el caso de los datos comprendidos y/o anejos a un correo electrónico.
- Siempre que vaya a desecharse cualquier documento o soporte que contenga datos personales deberá procederse a su destrucción o borrado, aplicando medidas que eviten el acceso a la información contenida en el mismo o su recuperación posterior.
- La implantación de medidas que garanticen la correcta identificación y autenticación de los usuarios deberá realizarse a partir de la entrada en vigor del Reglamento de desarrollo de la LOPD en todos los ficheros automatizados. Cuando dichos procesos se basen en contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. La periodicidad de las mismas no podrá ser superior a un año.
- Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos personales no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente y se anote su realización en el documento de seguridad. Previamente deberá haberse realizado una copia de seguridad.

5.3.2 Nuevas medidas de nivel básico

- El personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
- En los traslados se adoptarán medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información.
- La identificación de los soportes que contengan datos de carácter personal se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado identificar su contenido, y que dificulten la identificación para el resto de personas. Se admiten por tanto formas de etiquetado con códigos internos.
- Se permitirá la grabación de los datos manualmente solo en el caso de que la pérdida o destrucción afecte a ficheros o tratamientos parcialmente automatizados.
- El responsable del fichero deberá revisar cada seis meses la correcta definición de los procedimientos de copias de seguridad o *back-up*.

5.3.3 Nuevas medidas de nivel medio

Aunque se mantiene el plazo de máximo dos años para la realización de una auditoría de las medidas de seguridad, se prevé la obligación de auditar en caso de que se produzcan modificaciones sustanciales en los Sistemas de Información.

5.3.4 Nuevas medidas de nivel alto

No será necesario el registro de accesos en los siguientes supuestos:

- Cuando el responsable del fichero sea una persona física.
- Cuando el responsable del fichero garantice que únicamente él tiene acceso y trata los datos de carácter personal.

5.4 Ficheros no automatizados

Se encuentran reguladas en el Capítulo IV del Título VIII son las siguientes:

Se aplicarán a los ficheros no automatizados lo dispuesto por el Reglamento de desarrollo de la LOPD en lo relativo a:

- La aplicación de niveles de seguridad.
- La delegación de autorizaciones por parte del responsable del fichero.
- El régimen de trabajo fuera de los locales y así como el régimen de las copias de trabajo.
- El documento de Seguridad.
- Al Responsable de Seguridad
- A la obligación de someterse a una auditoría de carácter bienal para los ficheros sobre los que se apliquen las medidas de seguridad de nivel medio y alto.
- La determinación de funciones y obligaciones del personal.
- Al registro de incidencias, control de acceso y gestión de soportes y documentos.

Además de la aplicación de todas las estas medidas de carácter común para los ficheros automatizados y no automatizados, existen otras medidas específicas para los ficheros no automatizados:

- Cumplimiento de los criterios de archivo recogidos en la legislación específica de aplicación a cada caso o, en su defecto, obligación de establecer estos criterios para el archivo.
- Implantación de mecanismos de apertura en todos los dispositivos de almacenamiento.

Asimismo para aquellos ficheros que deban adoptar las medidas de seguridad de nivel Alto se prevé lo siguiente, en todo aquello relativo a su almacenamiento, que los armarios o archivadores que contengan datos de nivel alto en soporte no automatizado, deberán:

- Encontrarse en áreas con acceso protegido con puertas de acceso dotadas de sistemas de apertura mediante llave o dispositivo equivalente.
- Permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
- En caso de no ser posible la implantación de estas medidas, se adoptarán medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

- La generación de copias o la reproducción de estos documentos solo podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
- Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
- El acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
- El acceso de personas no autorizadas deberá quedar registrado de acuerdo con el procedimiento recogido en el documento de seguridad.
- Siempre que se proceda al traslado físico de la documentación, deberán adoptarse medidas para impedir el acceso o manipulación de la información.

En esencia estas son las novedades fundamentales respecto a la implantación de medidas de seguridad. Unas novedades que el legislador realiza con la intención de incrementar el nivel de protección de los datos de carácter personal y en donde es posible apreciar el gran esfuerzo realizado para tratar de adecuar la exigencia del principio de medidas de seguridad, establecido en el artículo 9 de la Ley Orgánica de Protección de Datos con el necesario establecimiento de un marco regulatorio más flexible que evite, al responsable del tratamiento, llevar a cabo un esfuerzo desproporcionado a la hora de implantar las medidas de seguridad en el seno de su organización.

CONCLUSIONES

I. Los factores tecnológicos, económicos y sociales han intervenido a aumentar los riesgos que el uso de las Tecnologías de la Información y las Comunicaciones pueden suponer para los derechos y libertades de las personas. En este sentido es necesario que la normativa, en materia de protección de datos de carácter personal, sea preventiva, de cara a minimizar el impacto que los avances tecnológicos y el desarrollo de la Sociedad de la Información, puedan tener en los citados derechos y libertades de las personas. Se hace totalmente necesario aprovechar el potencial de estos cambios como medio o instrumento que permita incrementar el conocimiento, la productividad, la competitividad sin que dichos fines supongan un menoscabo de los derechos y libertades de las personas. Esta simbiosis solo puede partir de una adecuada regulación que garantice que los derechos e intereses de los usuarios se vean adecuadamente protegidos. La protección de datos de carácter personal debe posicionarse como la primera salvaguarda contra los riesgos que los los nuevos modelos de sociales, económicos y tecnológicos pueden suponer para el ámbito más íntimo de la persona.

II. La propia naturaleza del derecho a la protección de datos de carácter personal se diferencia claramente del resto de derechos de la personalidad, recogidos en la Constitución Española y, por tanto, tal y como establece nuestro Alto Tribunal, el derecho a la protección de datos de carácter personal es un derecho fundamental de la personalidad de carácter autónomo, si bien es un derecho de elaboración *reciente*, que debe su forma final a la jurisprudencia del Tribunal Constitucional. En la actualidad podemos decir que se encuentra en un grado de madurez que permite proteger adecuadamente los bienes jurídicos en juego, aunque no por ello dejan de plantearse constantemente nuevos retos, debido fundamentalmente a los constantes cambios tecnológicos y sociales.

III: El derecho a la protección de los datos de carácter personal ha ido siguiendo un proceso de estandarización siendo esto especialmente significativo en el ámbito de la Unión Europea. La tendencia es sin duda a la unificación, tal y como lo demuestra la reciente propuesta europea para confeccionar un Reglamento de Protección de Datos, con eficacia directa en todo el territorio de la Unión lo cual derivará por un lado en una mejora de la protección de los derechos fundamentales de las personas, pero también en la garantía de que esta protección no interferirá en los flujos de información que cada vez en un mayor volumen son la base de la actividad económica a nivel global.

IV. Es de destacar la amplitud del marco normativo en la materia que nos ocupa, que afecta a un número creciente de áreas. La protección de datos personales es un factor a tener en cuenta en sectores tan dispares como las telecomunicaciones, la seguridad, las Administraciones Públicas, los servicios sanitarios y un largo etcétera. Dicho escenario supone que el estudio d ella protección de datos personales exige la revisión y análisis de un gran número de normas, tanto a nivel nacional como internacional. El ámbito de aplicación de una norma nos ayudará a determinar qué aspectos se van a ver afectados por las medidas reguladas en la misma y cuales quedan excluidas.

V. En líneas generales podemos decir que, en lo que al ámbito nacional se refiere, las líneas maestras, sobre las que se basa la protección de datos de carácter personal, se basan en el reconocimiento de tres conceptos clave:

- Dato personal, fundamentado de cualquier información personal referente a una persona identificada o identificable.
- Fichero, basado en la noción de finalidad.
- Tratamiento, como cualquier operación que se realice sobre datos personales organizados entorno a un fichero.

VI. Hemos tenido oportunidad de comprobar como la Ley Orgánica de Protección de Datos de Carácter Personal limita su aplicación en función del ámbito territorial en el que se desarrolle el tratamiento y como además se establecen regímenes especiales en función del tipo de fichero. En este sentido, la Ley Orgánica de Protección de Datos de Carácter Personal tan sólo resulta aplicable al tratamiento de datos personales relacionados con personas físicas. El fundamento de esta limitación del ámbito de aplicación reside en última instancia en la naturaleza de derecho fundamental de la protección de datos personales, no pudiendo entenderse que las personas jurídicas gocen del mismo en la misma medida que del derecho a la intimidad. De este modo, quedan excluidos de las garantías de la normativa aquellos datos que se refieran a personas jurídicas, debiéndose tener en cuenta en este sentido las reflexiones realizadas respecto a los datos de profesionales y empresarios individuales.

VII. Los principios esenciales, en una materia como la que nos ocupa, suponen una serie de aspectos imprescindibles para la protección del derecho de las personas y por lo tanto para la legitimación de los tratamientos que se lleven a cabo y que deberán garantizar en todo momento su cumplimiento. Los principios relativos a la calidad de los datos personales, a la información, el consentimiento, la finalidad de los tratamientos y a los datos especialmente protegidos se configuran como principios generales, en el sentido de que cualquier actuación sobre los datos personales debe respetarlos y adecuarse a ellos, pero de ellos también se derivan una serie de obligaciones concretas cuyo incumplimiento puede derivar en la imposición de sanciones. Mención especial merece el principio de confidencialidad o deber de secreto cuya principal misión consiste en salvaguardar o tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal y en definitiva el poder de control o disposición sobre sus datos. Su protección se garantiza obligando a los responsables de los tratamientos a establecer los medios que garanticen el cumplimiento de estas obligaciones por parte de todos aquellos que acceden a los datos personales en su nombre.

VIII. La firma de contratos de tratamiento de datos por encargo se ha convertido en una rutina entre empresas de prestación de servicios, que formalizan acuerdos que repiten textualmente el contenido del artículo 12 de la Ley Orgánica de Protección de Datos de Carácter Personal sin detenerse a valorar su importancia ni las obligaciones asumidas en los mismos. Sin embargo, es totalmente necesario conocer la normativa que se les impone a esta tipo de organizaciones y así lo han entendido especialmente aquellas entidades que demuestran interés en la normativa de protección de datos o que se encuentran en sectores de riesgos como pueden ser las telecomunicaciones, banca o los ficheros de morosos. Dichos responsables del tratamiento se han enfrentado en los últimos años a dos problemas a la hora cumplir las obligaciones recogidas en el artículo 12 de la Ley Orgánica de Protección de Datos de Carácter Personal:

- La prohibición de subcontratación de servicios.
- La obligación de destruir o devolver los datos tratados.

Por esta razón, la regulación del encargado del tratamiento ha sido matizada por la Agencia Española de Protección de Datos a través de consultas e informes jurídicos para adaptarla a la realidad práctica. Dichas matizaciones no parecían suficientes para contrarrestar la escasa importancia que el articulado de la Ley Orgánica de Protección de Datos de Carácter Personal confiere al encargado del tratamiento, que es, no podemos olvidarlo, sujeto de las sanciones recogidas en la ley junto al responsable del fichero. Por ello el Reglamento de desarrollo de la Ley

Orgánica de Protección de Datos de Carácter Personal confiere mayor relevancia a esta figura, con el objeto de poner fin a la situación arriba comentada y así lo refleja en su propio preámbulo:

*«(…)Se ofrece lo que no puede definirse sino como un **estatuto del encargado del tratamiento**, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el Título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado».*

Los puntos fundamentales de este "*estatuto"* del encargado del tratamiento son los siguientes:

- Se amplía la definición del artículo 3 de la Ley Orgánica de Protección de Datos de Carácter Personal, definiéndose al encargado del tratamiento como: *«La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará encargado del tratamiento a la persona o personas integrantes de los mismos».*
- Los artículos 20, 21 y 22, del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, están dedicados exclusivamente al responsable del tratamiento, recogiéndose en ellos el criterio mantenido por la Agencia en cuanto a subcontratación de servicio y conservación de datos.
- En relación al ejercicio de los derechos de acceso, rectificación, cancelación y oposición, se establece la obligación del encargado del tratamiento de trasladar la petición al responsable del fichero en plazos concretos ya que anteriormente se venía admitiendo que el encargado del tratamiento se limitara a contestar al interesado que no le correspondía atender su solicitud.
- Se incluyen previsiones específicas sobre medidas de seguridad que deberá adoptar el encargado del tratamiento.

IX. El régimen español para las transferencias internacionales de datos resulta complejo y farragoso. Combina un régimen de *"listas blancas"* de estados que garantizan la protección adecuada con una serie de requisitos que en ocasiones no son fáciles de aplicar.

Tanto la Instrucción 1/2000 como el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal han tratado de aclarar dicho régimen pero ambas normas no dejan a su vez de plantear dificultades, por lo que en la práctica muchas transferencias internacionales a países terceros tratan de buscar acomodo en las excepciones del artículo 34 de la Ley Orgánica de Protección de Datos de Carácter Personal, en particular, el consentimiento inequívoco del afectado, cuyo alcance, obtención y acreditación no está exento de problemas.

X. Las medidas de seguridad previstas en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal se configuran como un marco que pretende garantizar un tratamiento adecuado para todos los datos personales, independientemente del soporte en el que estos se encuentren o de la finalidad a la que se destinen. El cumplimiento del principio de seguridad es un requisito fundamental para determinar la legitimidad del tratamiento y por lo tanto, el cumplimiento de las medidas de seguridad atañe a todas las organizaciones, empresas e instituciones que almacenan y tratan datos de carácter personal en sus sistemas de información. El objetivo fundamental es que, en todo caso, los datos estén protegidos de cualquier posible incidencia que pueda provocar su pérdida, alteración o acceso no autorizado.

Este régimen ha evolucionado en los últimos tiempos con la entrada en vigor del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal. Se trata, de una evolución basada en la experiencia de los años de aplicación del Reglamento de Medidas de Seguridad y cuyos principales efectos se han dejado notar en dos facetas:

- Un incremento de las obligaciones que los responsables de ficheros deberán asumir. Este incremento ha venido definido por dos hechos: En primer lugar, algunas de las medidas que en el derogado Reglamento de Medidas de Seguridad se exigían exclusivamente para los ficheros de nivel medio y alto, se han trasladado también a los de nivel básico. Por otra parte, la regulación detallada de las medidas de aplicación a los ficheros de carácter no automatizado, va a implicar la aparición de nuevas obligaciones para estos responsables.
- *Adecuación de las obligaciones en función de las posibilidades reales de implantación de los responsables. En este sentido, el reconocimiento en muchos supuestos de la imposibilidad de implantar medidas concretas y la posibilidad, reconocida expresamente, de adoptar medidas alternativas que se justifiquen adecuadamente en el Documento de Seguridad, debe implicar la adaptación de estas obligaciones a las posibilidades de*

responsables de ficheros con menos posibilidades técnicas y organizativas.

BIBLIOGRAFÍA

I. LEGISLACIÓN Y JURISPRUDENCIA

Asamblea General de las Naciones Unidas (1990). Resolución 45/95, de 14 de diciembre de 1990, relativa a los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales

Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 15 de junio de 2005. Recurso 669/2003.

Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 15 de marzo de 2002. Recurso 271/2001.

Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 16 de Febrero 2006. Recurso 511/2004

Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 7 Julio de 2000. Recurso 121/1999.

Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 8 de febrero de 2006. Recurso 495/2004.

Boletín Oficial de las Cortes Generales (1999). Informe de la Comisión Especial de Redes Informáticas del Senado. Aprobado por acuerdo del Pleno del Senado en su sesión del día 17 de diciembre de 1999. Senado, número 812, de 27 de diciembre.

Comisión de las Comunidades Europeas. Decisión de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Publicada el 25 de agosto de 2000 en el Diario Oficial de las Comunidades Europeas, número L 215.

Comisión de las Comunidades Europeas. Decisión de la Comisión de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection). Publicada el 6 de julio de 2004 en el Diario Oficial de las Comunidades Europeas, número L 235.

Comisión de las Comunidades Europeas. Decisión del Consejo de 17 de mayo de 2004 relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos. Publicada el 20 de mayo de 2004 en el Diario Oficial de las Comunidades Europeas, número L 183.

Consejo de Europa (1997). Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos.

Consejo de Europa. Convenio 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Consejo de Europa. Recomendación R (74) 29. Relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.

Consejo de Europa. Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

Diario Oficial de la Unión Europea (2002). Serie L. Decisión del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia. Número 63. Marzo de 2002.

Diario Oficial de la Unión Europea. Serie C. Acto de la Autoridad Común de Control de Eurojust de 2 de marzo de 2004 por el que se establece su Reglamento interno. Número 86. Abril de 2004.

Jefatura del Estado. Instrumento de Ratificación del Acuerdo entre el Estado español y la Santa Sede sobre Asuntos Jurídicos, firmado en la Ciudad del Vaticano el 3 de enero de 1979. Publicada en el Boletín Oficial del Estado n.º 300, de 15 de diciembre de 1979.

Jefatura del Estado. Ley 2/2011, de 4 de marzo, de Economía Sostenible. . Publicada en el Boletín Oficial del Estado n.º 55, de 5 de marzo de 2011.

Jefatura del Estado. Ley 23/1992, de 30 de julio, de Seguridad Privada. Publicada en el Boletín Oficial del Estado n.º 186, de 04 de agosto de 1992.

Jefatura del Estado. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Publicado en el Boletín Oficial del Estado n.º 251 de 19 de octubre de 2007.

Jefatura del Estado. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Publicada en el Boletín Oficial del Estado n.º 166, de 12 de julio de 2002.

Jefatura del Estado. 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. Publicada en el Boletín Oficial del Estado n.º 274, de 15 de noviembre de 2002.

Jefatura del Estado. Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Publicada en el Boletín Oficial del Estado número 262 de 31 de octubre de 1992

Jefatura del Estado. Ley Orgánica 14/2003, de 20 de noviembre, de Reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, modificada por la Ley Orgánica 8/2000, de 22 de diciembre; de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local; de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y de la Ley 3/1991, de 10 de enero, de Competencia Desleal. Publicada en el Boletín Oficial del Estado número 279 de 31 de noviembre de 2003.

Ministerio de Justicia e Interior. Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Publicado en el Boletín Oficial del Estado n.º 147 de 21 de junio de 1994.

Ministerio de Justicia. Real Decreto 994/1999 Reglamento de Medidas de Seguridad de los ficheros automatizados. Publicado en el Boletín Oficial del Estado n.º 151 de 25 de junio de 1999.

Parlamento Europeo, Consejo. 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. Publicado en Doce N.º L 281, 23 de noviembre de 1995.

Presidencia de la Generalidad de Cataluña. Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos. Publicado en el Diario Oficial de la Generalidad de Cataluña número 3625, de 29 de abril de 2002.

Presidencia del Gobierno. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Publicado en el Boletín Oficial del País Vasco número 44, de 04 de marzo de 2004.

Secretaría General Técnica de Vicepresidencia, Consejería de Cultura y Deporte y Portavocía del Gobierno. Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. Publicada en el Boletín Oficial de la Comunidad de Madrid, de 25 de julio de 2001.

Tribunal Constitucional, Pleno, Sentencia 228/2003 de 18 de diciembre de 2003, Recurso 3342/1995.

Tribunal Constitucional, Pleno, Sentencia 290/2000 de 30 de noviembre de 2000. Recurso 201/1993.

Tribunal Constitucional, Pleno, Sentencia 292/2000 de 30 de noviembre de 2000. Recurso 1463/2000.

Tribunal Constitucional, Sala Primera, Sentencia 254/1993 de 20 Julio de 1993, recurso 1827/1990.

Tribunal Constitucional. Pleno. Sentencia 154/2002, de 18 de julio.

Tribunal Constitucional. Sala Primera. Sentencia 11/1998, de 13 de enero.

Tribunal Constitucional. Sala Primera. Sentencia 110/1984, de 26 de noviembre.

Tribunal Constitucional. Sala Primera. Sentencia 143/1994, de 9 de mayo.

Tribunal Constitucional. Sala Primera. Sentencia 214/1991, de 11 de noviembre.

Tribunal Constitucional. Sala Primera. Sentencia 254/1993, de 20 de julio.

Tribunal Constitucional. Sala Segunda. Sentencia 156/2001, de 2 de julio. Fundamento Jurídico Tercero.

Tribunal Constitucional. Sala Segunda. Sentencia 231/1988, de 2 de diciembre-

Tribunal Constitucional. Sala Segunda. Sentencia 197/1991, de 17 de octubre.

Tribunal Constitucional. Sala Segunda. Sentencia 57/1994 de 28 de febrero.

Tribunal Constitucional. Sala Segunda. Sentencia 94/1998, de 4 de mayo.

Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-administrativo, Sección 8ª, Sentencia de 10 de mayo de 2000. Recurso 1513/1997.

Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-administrativo, Sección 8ª, Sentencia de 17 de mayo de 2001. Recurso 724/1998.

Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-administrativo, Sección 9ª, Sentencia de 30 de enero de 2003. Recurso 1856/1997.

Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 6ª, Sentencia de 20 de febrero de 2007. Recurso 732/2003.

Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 7ª, Sentencia de 26 de septiembre de 2005. Recurso 4673/1999.

II. ARTÍCULOS Y LIBROS

ALMUZARA ALMAIDA, C. (Coord.) (2005). Estudio Práctico sobre la protección de datos de carácter personal. Editorial Lex Nova. Valladolid.

APARICIO SALOM, J. (2000). Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Editorial Aranzadi. Elcano (Navarra).

CARRASCO LINARES, J. y PUENTE SERRANO, N (2004). Las relaciones entre empresas, La Protección de Datos en la Gestión de Empresas. Editorial Thompson Aranzadi. El Cano (Navarra).

CARRERAS SERRA, L. (2003). Derecho Español de la Información. UOC. Universitat Oberta de Catalunya.

CARRETERO SÁNCHEZ, S. (2005). Nueva introducción a la Teoría del Derecho. Madrid: Dykinson.

CASTÁN TOBEÑAS, J. (1979). Los derechos del hombre. Prólogo de Luis Legaz Lacambra. Reus. Madrid.

CONDE ORTIZ, C. (2005). La protección de datos personales. Dykinson.

CORRIPIO, M. R. (2002). Novedades Legislativas sobre protección de datos. La Directiva 2002/58/CE. Revista de Contratación Electrónica. Número. 32. Noviembre de 2002

CUADRADO GAMARRA, N. (2005). Capacidad jurídica y derechos subjetivos en relación con las Nuevas Tecnologías. En La capacidad Jurídica. Madrid: Dykinson.

DAVARA RODRÍGUEZ, M. (2006). Manual de Derecho Informático 8ª Edición. Thomson Aranzadi.

DEL PESO NAVARRO, E. y RAMOS GONZÁLEZ, M.A. (1998): LORTAD, Análisis de la Ley. Ediciones Díaz de Santos. Madrid.

DEL PESO NAVARRO, Emilio (2000). Ley de Protección de Datos: la nueva LORTAD. Editorial Díaz de Santos. Madrid.

GUERRERO PICÓ, M. (2005). El derecho fundamental a la protección de datos de carácter personal en la Constitución Europea. ReDCE número 4. Julio-Diciembre.

GÓMEZ NAVAJAS, J. (2005). La protección de datos personales. Un análisis desde la perspectiva del derecho penal. Thomson Civitas. Madrid.

HEREDERO HIGUERAS, M. (1997). La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento

de los datos personales y a la libre circulación de estos datos. Editorial Aranzadi. Elcano (Navarra).

HERRAN ORTIZ, A. (2003), La protección de datos sanitarios. Especial referencia a la Ley 41/2002, de 14 de noviembre, reguladora de los derechos. Revista de Derecho VLex, número 12, diciembre de 2003.

HERRAN ORTIZ, A. (2002). El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales. Dykinson. Madrid.

LUCAS MURILLO P. (2005). Texto de la conferencia que tuvo lugar el 24 de octubre de 2005 en la sede de la Agencia Catalana de Protección de Datos [En línea]. Disponible en :www.apd.cat [2011, 10 de enero]

MAESTRE RODRÍGUEZ, J.A. (2003). La intimidad: El derecho de autodeterminación personal. En Nuevas Tecnologías de la Información y Derechos Humanos. Cedecs.

MARTÍNEZ SANCHEZ, M. (2001): Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Universidad Pontificia de Comillas. XIV Encuentros sobre Informática y Derecho 2000-2001. Editorial Aranzadi. Madrid.

MARTÍNEZ SÁNCHEZ, M. (2000). Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. AJA, número 35.

MARZO PORTERA, A. y MACHO-QUEVEDO, A. (2004): La Auditoría de Seguridad en la Protección de Datos de Carácter Personal. Ediciones Experiencia. Barcelona.

MENÉNDEZ MATO, J.C. (2005). El contrato vía Internet. Bosch.

MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto (2000). La cesión o comunicación de datos de carácter personal. Editorial Thompson Civitas. gencia de Protección de Datos de la Comunidad de Madrid. Madrid.

MURILLO DE LA CUEVA. P. L. (1990). El Derecho a la Autodeterminación Informativa. La Protección de Datos Personales frente al Uso de la Informática. TECNOS. Madrid.

MÁRQUEZ LOBILLO P. (2004). Empresarios y profesionales en la sociedad de información. Edersa, 2004.

PIÑAR MAÑAS, J. (2008): «Novedades en relación con la figura del Encargado del Tratamiento» en «Protección de Datos. Comentarios al Reglamento». Editorial Lex Nova. Valladolid.

PIÑAR MAÑAS, J.L. (2006). Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal. En Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch/Agencia Española de Protección de Datos/Red Iberoamericana de Protección de

Datos.

PUJOL MONTERO, J. (2007): “El derecho de acceso”, Obra colectiva: «La Protección de Datos (I)». Boletín del Ilustre Colegio de Abogados de Madrid. Número 35, 3ª época, febrero de 2007.

REBOLLO DELGADO, L. (2004) Difusión a través de Internet de infracciones penales o administrativas, sin consentimiento de los interesados. Revista Datos Personales, Número 9, Mayo de 2004.

SANCHEZ MOURIZ, Nelly (2004). Los datos personales en el inicio de una actividad empresarial. La Protección de Datos en la Gestión de Empresas. Editorial Thompson Aranzadi. Cizur Menor (Navarra).

SANCHO VILLA, D. (2003). Transferencia Internacional de Datos Personales. Agencia Española de Protección de Datos. Madrid.

SANTAMARÍA RAMOS, F.J. (2011). El encargado independiente. Figura clave para un nuevo derecho de protección de datos. Madrid: Wolters Kluwer España.

SERRANO PÉREZ, M. (2003): El derecho fundamental a la protección de datos. Derecho español y comparado. Thomson Civitas. Madrid.

SERRANO PÉREZ., M. (2005): “El derecho fundamental a la protección de datos. Su contenido esencial”. Los derechos fundamentales y las nuevas tecnologías. Anuario multidisciplinar para la modernización de las administraciones públicas. Nº 1, Año 2005. Disponible en http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/home.jsp

SUÑÉ LLINAS, E. (1999). TRATADO DE DERECHO INFORMÁTICO. INTRODUCCIÓN Y PROTECCIÓN DE DATOS PERSONALES (VOLUMEN I; 2ª EDICIÓN). MADRID: SERVICIO DE PUBLICACIONES DE LA FACULTAD DE DERECHO. UNIVERSIDAD COMPLUTENSE DE MADRID.

TOURIÑO TROITIÑO, M. (2007): Datos de Carácter Personal - Medidas de protección para ficheros automatizados en el borrador del Reglamento de la Ley 15/99. Revista Datos Personales de 28 Julio 2007.

TRONCOSO REIGADA, A. (2007): “La protección de datos personales en las administraciones públicas”. Obra colectiva: «La Protección de Datos (I)». Boletín del Ilustre Colegio de Abogados de Madrid, número 35, 3ª época. Febrero.

ULL PONT, E. (2003). Derecho Público de la Informática. Protección de Datos de Carácter Personal. 2ª edición actualizada, UNED Ediciones. Madrid.

III. MEMORIAS

Agencia Española de Protección de Datos. Memoria del año 1994 [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_1994/common/pdfs/MemoriaApd1994.pdf

Agencia Española de Protección de Datos. Memoria del año 1994, [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2002/common/pdfs/MemoriaApd1994.pdf

Agencia Española de Protección de Datos. Memoria del año 1999, [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_1999/common/pdfs/MemoriaApd1999.pdf

Agencia Española de Protección de Datos. Memoria del año 2000 [en línea]. Madrid. Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2000/common/pdfs/MemoriaApd2000.pdf

Agencia Española de Protección de Datos. Memoria 1999 [en línea]. Disponible en: http://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2003/common/pdfs/MemoriaApd1999.pdf

Agencia Española de Protección de Datos. Memoria 2005 [en línea]. Disponible en: http://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2005/common/pdfs/8290-CAP.IV-Csdigos-Tipo.pdf

IV. INFORMES

Agencia Española de Protección de Datos (1995). «Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.»

Agencia Española de Protección de Datos (2000). Informe jurídico 0000/2000 sobre tratamiento por Abogados y Procuradores de los datos de las partes en un proceso.

Agencia Española de Protección de Datos (2001). Informe jurídico 0000/2001 sobre el bloqueo de datos de carácter personal.

Agencia Española de Protección de Datos (2002). Informe 0042/2002.

Agencia Española de Protección de Datos (2002). Informe jurídico sobre el ejercicio del derecho de acceso por los herederos del afectado.

Agencia Española de Protección de Datos (2003). Informe jurídico 189/2003 sobre cancelación de datos contenidos en historias clínicas.

Agencia Española de Protección de Datos (2003). Informe jurídico 534/2003 sobre el cómputo del plazo para la satisfacción de los derechos de rectificación y cancelación

Agencia Española de Protección de Datos (2004). Informe 0000/2001: Distinción entre ficheros de titularidad pública y privada [en línea].

Agencia Española de Protección de Datos (2004). Informe 0283/2004. Conservación de los datos por el encargado del tratamiento.

Agencia Española de Protección de Datos (2004). Informe 0416/2004. Naturaleza de encargado del tratamiento del prestador de servicios de housing.

Agencia Española de Protección de Datos (2004). Informe 0582/2004. Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable.

Agencia Española de Protección de Datos (2004). Informe jurídico 0409/2004 sobre acceso por el titular de la patria potestad a las historias clínicas de los menores.

Agencia Española de Protección de Datos (2005). Informe 0026/2005: Transmisión de datos dentro de la Unión Europea.

Agencia Española de Protección de Datos (2005). Informe 0334/2005: Tratamiento de datos realizados a bordo de buques.

Agencia Española de Protección de Datos (2005). Informe jurídico 0049/2005 sobre el derecho de cancelación sobre los datos de un paciente.

Agencia Española de Protección de Datos (2005). Informe jurídico 0167-2005 sobre la naturaleza y alcance del derecho de acceso

Agencia Española de Protección de Datos (2006). Informe 0119/2006: Cesión de datos de facturación de las oficinas de farmacia.

Agencia Española de Protección de Datos (2006). Informe 365/2006: «Tratamiento y cesión de datos de personas fallecidas».

Agencia Española de Protección de Datos (2006). Informe 425/2006: Matrículas de vehículos y concepto de dato de carácter personal.

Agencia Española de Protección de Datos (2007). Informe 0020/2007 [en línea]. Cumplimiento del deber de información.

Agencia Española de Protección de Datos (2007). Informe 0049/2007.

Agencia Española de Protección de Datos (2007). Informe 0055/2007. Comunicación de datos de compradores.

Agencia Española de Protección de Datos (2007). Informe jurídico 0252/2007 sobre cuestiones de videovigilancia y ejercicio de derechos.

Agencia Española de Protección de Datos (2007). Informe jurídico 0379/2007 sobre acceso a datos del padrón por particulares.

Agencia Española de Protección de Datos (2008). Informe 0156/2008: Medidas de seguridad en los ficheros de nóminas y demás especialidades.

V. WEBGRAFÍA

Agencia Catalana de Protección de Datos: www.apdcat.net

Agencia Española de Protección de Datos: www.agpd.es

Agencia Vasca de Protección de Datos: www.avpd.euskadi.net/s04-4319/es/

Agencia de Protección de Datos de la Comunidad de Madrid:

Autoridad Común de Control de Europol: http://europoljsb.ue.eu.int/default.asp?lang=ES

Autoridad Común de Control de Shengen: www.schengen-jsa.dataprotection.org

Comisión Europea: http://europa.eu.int

Consejo UE: http://ue.eu.int

Consejo de Europa: www.coe.int

Estados Unidos -Departamento de Seguridad Interior-: www.dhs.gov

Estados Unidos -FTC, en castellano-: www.ftc.gov/ftc/spanishinfo/consumer.htm

Grupo del art. 29:http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

Information Systems Audit and Control Association (www.isaca.org)

Propuesta de Reglamento General de Protección de Datos. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

www.madrid.org/apdcm

VI. OTROS

Agencia Española de Protección de Datos (1995). Instrucción 1/1995, de de 1 de marzo, de la Agencia Española de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y de crédito.

Agencia Española de Protección de Datos (1996). «Instrucción 1/1996, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios».

Agencia Española de Protección de Datos (1998). «Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.».

Agencia Española de Protección de Datos (2000). «Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos».

Agencia Española de Protección de Datos (2004). Plan de inspección de oficio a cadenas hoteleras. Conclusiones y recomendaciones.

Agencia Española de Protección de Datos (2005). Resolución de 19 de julio de 2005.

Agencia Española de Protección de Datos (2005). Resolución de 24 de agosto de 2005.

Agencia Española de Protección de Datos (2005). Resolución de 31 de mayo de 2005.

Agencia Española de Protección de Datos (2006). Resolución de 9 de mayo de 2006.

Agencia Española de Protección de Datos (2007). Resolución de 15 de junio de 2007.

Agencia Española de Protección de Datos (2007). Resolución de 20 de noviembre de 2007.

Agencia Española de Protección de Datos (2008). Resolución de 10 de marzo de 2008.

Agencia Española de Protección de Datos (2008). Resolución de 11 de enero de 2008.

Agencia Española de Protección de Datos (2008). Resolución de 25 de febrero de 2008.

Agencia Española de Protección de Datos (2008). Resolución de 28 de febrero de 2008.

Agencia Española de Protección de Datos (2008). Resolución de 5 de marzo de 2008.

Agencia Española de Protección de Datos. Inspección sectorial de oficio "Concursos, juegos y sorteos de televisión". Conclusiones y Recomendaciones. Octubre de 2002.

Agencia de Protección de Datos de la Comunidad de Madrid: «Los datos publicados en Diario Oficial, a través de formato electrónico, podrán cancelarse cuando haya desaparecido la causa que motivó su publicación».

Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, celebrada en Cracovia del 25 al 26 de abril de 2005. Agencia de Protección de Datos de la Comunidad de Madrid (2008) .Revista Datos Personales en su ejemplar de Enero.

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad..pdf

Grupo de trabajo del artículo 29 (1998). Transferencias de datos personales a terceros países: Aplicación de los artículos 25 y 26 de ña Directiva sobre protección de datos de la Unión Europea.

Recomendaciones de la Agencia Española de Protección de Datos al Sector del Comercio

Electrónico para la adecuación de su funcionamiento a la LOPD, publicada en la Memoria anual correspondiente al año 2000