

Esta sección, pretende ser una puerta abierta a la comunicación entre los colegiados, y está a disposición de todos los integrantes del Ilustre Colegio de Abogados de Valladolid, para que nos trasladéis vuestras experiencias e inquietudes, a cuyo fin ponemos a vuestra disposición la dirección de correo electrónico de “abogados de Valladolid”: revista@icava.org

LA LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Por **SOCORRO BARRERO. Colegiado ICAVA.**

La ya conocida aunque no muy aplicada Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) establece en su artículo 1: *“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”,* señalando en su artículo 3 a) que se entenderá por datos de carácter personal *“cualquier información concerniente a personas físicas identificadas o identificables”*.

En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento 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 profesionales y a la libre circulación de estos datos.

Como Ley Orgánica que es, regula la protección de un derecho fundamental, en este caso el establecido en el artículo 18.4 CE: *“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”,* consagrándose así el derecho a la protección de datos como un derecho autónomo, incluso del propio derecho a la intimidad, tal y como

ha indicado la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, dentro de lo que se ha dado en llamar *“libertad informática”* o *“autodeterminación informática”*.

El derecho fundamental a la protección de datos es más amplio que el derecho fundamental a la intimidad consagrado en el art. 18.1 de la CE, pues no sólo protege la intimidad de las personas sino que también protege aspectos de la vida que afectan a reputación y a la esfera privada de cada ciudadano, de ahí que lo que se protege no son sólo datos íntimos, sino cualquier clase de dato que pueda afectar a cualesquiera de sus derechos sean o no fundamentales, sus libertades, su honor y pleno disfrute de los restantes derechos.

Se concreta este derecho fundamental en la capacidad de todo ciudadano de controlar los datos relativos a su persona y difiere respecto al derecho fundamental a la intimidad del art. 18.1 en que la función de este último es la de proteger la intimidad, aquéllo que cualquier persona desea excluir del conocimiento público o ajeno frente a una eventual invasión de terceros, y la función del derecho fundamental de protección de datos es garantizar a cada persona un poder de control sobre sus datos personales, sobre su uso y destino,

con el propósito de impedir un tratamiento ilícito que afecte a su dignidad y a sus derechos. En definitiva el poder de disposición sobre sus datos.

Incardinada en este precepto constitucional nació la LO 5/92, de 29 de octubre de Regulación Del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) refiriéndose a los ficheros automatizados de datos de carácter personal tanto de titularidad pública como privada, hoy derogada por la LOPD (Disposición Derogatoria Única).

Pues bien, la LOPD cuyo objeto es garantizar ese derecho fundamental a la protección de datos, se sustenta sobre dos pilares: el de los principios de protección de datos (Título II) y el de los derechos de las personas (Título III).

En ellos se regula precisamente ese poder jurídico que tienen las personas respecto a sus datos, de esa facultad que tienen de exigir a terceros una conducta activa u omisiva respecto de aquéllos, que garantiza la salvaguarda de este derecho fundamental

El título II (Arts. 4 a 12) impone a los titulares de ficheros unas obligaciones tendentes a garantizar este derecho fundamental, regulando su ejercicio mediante un conjunto de garantías que hacen posible el

respeto al mismo y que se concretan en los principios de calidad de los datos, información a los sujetos titulares sobre su origen y destino, y el consentimiento para su uso y cesión.

El Título III (Arts. 13 a 19) completa ese conjunto de garantías concediendo a los sujetos titulares de los datos las facultades de acceso, oposición, rectificación y cancelación de los datos, e igualmente concede a los afectados un eventual derecho indemnizatorio

El ámbito de aplicación se regula en el 2.1 de la LOPD establece: *“La presente Ley 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 esos datos por los sectores público y privado”.*

Por soporte físico hemos de considerar no solo los ficheros automatizados sino a los creados en soporte papel.

El art. 2.2 contiene las exclusiones que se refieren únicamente a los ficheros de personas físicas en el ámbito personal y doméstico, a los ficheros protegidos por la normativa de de materias clasificadas y aquéllos creados para la investigación del terrorismo y de formas graves de delincuencia organizada.

Examinaremos ahora con más detenimiento el conjunto de garantías en que informan la LOPD

TÍTULO II

El principio de calidad de los datos se regula en el art. 4. Dicho principio obliga a los titulares de ficheros a que los datos que se hayan de obtener sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para la que se obtienen. En consecuencia no se pueden exigir ni solicitar más datos que aquéllos estrictamente necesarios para los fines pretendidos, finalidades que además han de ser determinadas –no genéricas-, explícitas –el afectado ha de conocerlas-, y por supuesto legítimas, con la prohibición expresa al titular del fichero de recabar esos datos con medios fraudulentos, desleales o ilícitos y de usar esos datos para



finés incompatibles con la finalidad con la que se obtuvieron.

Impone además el legislador otra obligación al titular del fichero que consiste en mantener los datos exactos y puestos al día, de tal modo que reflejen la real situación del afectado. De no ser así habrá de cancelarlos de oficio y sustituirlos por los datos exactos. Fijémonos en un sencillo ejemplo para destacar la relevancia de este aspecto: en los ficheros de morosos la inexactitud de un dato de naturaleza económica puede tener como consecuencia directa que a una persona le concedan o no un crédito.

Otra de las obligaciones derivadas de este principio se refiere a la conservación y almacenamiento de los datos que solo podrán realizarse mientras las mismas sean necesarias para cumplir los fines con que fueron obtenidos, tras lo cual habrán de ser cancelados.

El artículo 5 regula el derecho de información en el proceso de recogida de los datos. Este principio es especialmente importante porque determinará con posterioridad si el consentimiento prestado

para la recogida y tratamiento de los datos reúne los requisitos exigidos por la Ley.

Establece la Ley que los interesados de los que se trate de obtener datos personales habrán de ser previamente informados de modo expreso preciso e inequívoco de la existencia de un fichero, de la finalidad de la recogida de los datos y de los destinatarios de esos datos, de la identidad y domicilio del responsable del fichero, del carácter obligatorio o facultativo de las respuestas a las preguntas que se les formulen y de las consecuencias en su caso de la negativa a responder; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Si además dicha recogida se hace mediante cuestionario o impreso, éstos deberán contener todos estos requisitos.

Las excepciones a este principio son únicamente cuando una ley así lo prevea y cuando de la naturaleza o circunstancias de los datos que se solicitan se infiere el contenido de aquellos requisitos

El artículo 6 regula el consentimiento del afectado, siendo este principio el que recoge y contempla más ampliamente esa



¿Necesita ayuda con la Protección de Datos?



Adapte ya su despacho a las exigencias legales sobre protección de datos o solicite información sobre las posibilidades de colaboración para la implantación del sistema a sus clientes.

Pónganse en contacto con nosotros en el teléfono **983 217 804** o por correo electrónico: **protecciondedatos@eurosl.es** y le informemos con más detalle.



EURO S.L.
Asesoramiento y consultoría empresarial

GRUPO

AFYC



www.eurosl.es

C/Santiago, 13-3ªA
47001 VALLADOLID
Tfno.: 983 340 865

C/Oro, 42- 1ºIzq. Pol. de San Cristóbal
47012 VALLADOLID
Tfno.: 983 217 804

C/Ignacio Mtnez. de Azcoitia, 1-3º
34001 PALENCIA
Tfno.: 979 706 106

autodeterminación informática o libertad informática que constituye el art. 18.4 de la CE.

El art. 6.1 establece: *“El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado salvo que la Ley disponga otra cosa”* y el art. 3.h) de la Ley define el consentimiento del interesado como *“toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”*. Del estudio de ambos preceptos se infiere que es necesario que concurren estos cuatro requisitos para que el consentimiento sea prestado válidamente.

La Agencia Española de Protección de Datos ha interpretado estas cuatro características manifestando que el consentimiento conforme a derecho habrá de ser:

- 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 precitado artículo 4.2 de la LOPD.
- 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 LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen y que antes hemos analizado.
- 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.

Una duda muy frecuente es si el consentimiento ha de ser siempre expreso o puede ser tácito: pues bien; cuando el legislador ha querido que fuera expreso así lo ha indicado, y eso sucede en el caso

de tratamiento de los datos especialmente protegidos del art. 7 en el que se distinguen datos para cuyo tratamiento es necesario el consentimiento previo no solo expreso sino escrito, tal es el caso del art. 7.2: ideología, religión, creencias y afiliación sindical y datos para cuyo tratamiento exige el consentimiento expreso pero no escrito, cual es el caso del art. 7.3: salud, el origen racial y la vida sexual.

Por lo tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3), si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo.

El art. 6 regula en su punto segundo las excepciones al consentimiento del afectado para el tratamiento de sus datos:

- Cuando se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias
- Cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su cumplimiento o mantenimiento.
- Cuando el tratamiento tenga por finalidad proteger un interés vital del interesado
- Cuando los datos se recaben de fuentes accesibles al público, siempre que no se vulneren derechos y libertades del afectado.

El artículo 9 regula la Seguridad de los datos e impone a los titulares de ficheros la obligación de garantizar la seguridad de los datos, de evitar su alteración, pérdida, y tratamientos o accesos no autorizados, mediante la adopción de las medidas necesarias tanto de índole técnica como organizativa.

El Real Decreto 994/1999, de 11 de julio por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carác-



ter personal, contiene en su articulado los requisitos mínimos exigidos para garantizar lo previsto en el art. 9.

El art. 10 regula el deber de secreto que tienen tanto los responsables de ficheros que contengan datos de carácter personal así como todos los intervinientes en cualquier fase del tratamiento de aquéllos previendo expresamente que dicha obligación subsistirá aun cuando acabe el tratamiento de los datos.

En relación con el poder de control que cada persona tiene sobre sus datos que se va reflejando en los preceptos ya analizados respecto al derecho de información del afectado, a la necesidad de su consentimiento para tratar los datos y al deber de secreto impuesto a todos los intervinientes en cualquier fase del tratamiento, se regula la cesión o comunicación de datos en el art. 11 que establece: *“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”*. Dicho consentimiento es en cualquier caso revo-



cable y es otra de las manifestaciones del ejercicio del derecho fundamental a la protección de datos, del poder de disposición que cada persona tiene sobre sus datos, teniendo como finalidad el que los éstos no se divulguen a terceros distintos a quienes se les facilitó con las negativas consecuencias que de su ilícito uso puedan derivarse.

Este principio admite excepciones cuando una ley lo prevea, como consecuencia de una relación jurídica libremente aceptada por las partes, por motivos de orden público, por razones de urgencia por motivos de salud y como consecuencia de estudios epidemiológicos.

El art. 12 regula el llamado acceso a los datos por cuanta de terceros estableciendo que no se considera 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 tratamiento, relación que deberá ser regulada en un contrato en el que, entre otras, se estipularán las medidas de seguridad a que se refiere el art. 9.

Aunque no lo establece el precepto, el contrato ha de constar necesariamente por escrito.

Como hemos visto en este bloque de principios se regulan los requisitos para que el tratamiento de los datos respete el derecho fundamental a su protección, de manera que se imponen determinadas conductas a los responsables o titulares de ficheros de datos en orden a garantizar tal derecho.

TÍTULO II

En cuanto al segundo pilar en que se sustenta la Ley, sistematizado en el Título II, como hemos dicho es el bloque de derechos de los afectados, interesados o sujetos titulares de datos, derechos que despliegan sus efectos en la facultad que las personas poseen de saber quién tiene sus datos, de exigir del titular del fichero que le informe de qué datos posee sobre su persona accediendo a los oportunos registros y asientos y qué destino han tenido, lo que alcanza también a posibles cesionarios, e igualmente la facultad de oponerse a su tratamiento y, en su caso, requerir al responsable del fichero para que los rectifique

o cancele. También se regulan en este título las condiciones para el ejercicio de estos derechos, para los que no se exigirá contraprestación alguna (art. 17).

Todos estos derechos se concretan de la siguiente manera:

- Derecho de consulta al Registro General de Protección de Datos para saber de la existencia de tratamientos de datos, de sus finalidades y del responsable del tratamiento o fichero (art. 14).
- Derecho de acceso (art. 15), que consiste en la facultad que tiene el interesado de solicitar y obtener del responsable del fichero de forma gratuita o no muy costosa (carta, fax,...) información sobre sus datos sometidos a tratamiento, el origen de los mismos así como las comunicaciones o cesiones tanto realizadas como previstas.

Este derecho sólo podrá ejercitarse a intervalos no inferiores a doce meses salvo que se acredite un interés legítimo

- Derecho de rectificación y cancelación (art. 16), requiriendo al responsable del fichero para que rectifique o cancele los datos, teniendo obligación el responsable de realizarlo en el plazo de diez días.

El artículo 18 establece que la denegación total o parcial de estos derechos por parte del responsable del fichero podrá ser motivo de denuncia por parte de los interesados ante la Agencia de Protección de Datos quien, en ejercicio de sus funciones de tutela de derechos, resolverá en un plazo máximo de seis meses sobre la procedencia o improcedencia de la denegación mediante un resolución expresa, contra la que, en su caso, se podrá interponer recurso contencioso-administrativo.

Finalmente el art. 19 prevé un eventual derecho indemnizatorio para el caso de que los interesados sufran lesión en sus bienes o derechos como consecuencia de la no observancia de esta Ley por parte del responsable del fichero. Esta acción se ejercitará ante la jurisdicción ordinaria en el caso de que los ficheros sean de titularidad privada, siendo de aplicación lo previsto en el régimen de responsabilidad de las administraciones públicas cuando se trate de ficheros de titularidad pública.