capítulo sexto

Protección de datos en la empresa

1. INTRODUCCIÓN

Actualmente las empresas no pueden prescindir, para llevar su gestión, de acudir a un tratamiento automático de la información utilizando la potencialidad de la informática e, incluso, de la informática más las comunicaciones. La gestión de los recursos, la prestación de servicios, la toma de decisiones, así como las funciones, entre otras, de planificación y control, obligan a manejar muchos datos, y esto no es posible sin su tratamiento mediante las Tecnologías de la Información y las Comunicaciones (TIC).

En muchos casos, los gestores de recursos ajenos se encuentran ante la necesidad del conocimiento de diferentes tipos de datos e informaciones de las personas para realizar con eficacia su gestión o controlar aquellos aspectos orientados al cumplimiento de objetivos de interés común.

El tratamiento automatizado de la información no está exento de riesgos y peligros entre los que se muestra como preferente atender al respeto debido a las personas ante el derecho fundamental de nueva creación que se ha dado en denominar "derecho fundamental a la protección de datos" [69].

Entenderemos por protección de datos "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".

Los archivos y registros de datos de personas –con las que la empresa mantiene una relación contractual, laboral, de cliente, proveedor, económica, social u otras–, se encuentran, generalmente, en soportes automatizados, o susceptibles de tratamiento automatizado, a los que se puede acceder mediante un programa de recuperación de información por determinados parámetros, bajo la forma y estructura conocida de las bases de datos, lo que facilita su recuperación y consulta y proporciona

[69] *La Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional, estimando el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo, contra los artículos 21.1 y 24.1 y 2 de la LOPD, claramente indica que el "derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad ... 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 ..." (último párrafo del Fundamento Jurídico 5). Así como también lo señala el artículo 8 de la Carta de los derechos fundamentales de la Unión Europea de 7 de diciembre de 2000 (2000/C 364/01), cuando dice: "Artículo 8. Protección de datos de carácter personal: Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados 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. El respeto de estas normas quedará sujeto al control de una autoridad independiente".*

una agilidad y dinámica a su tratamiento[70]; los parámetros de recuperación suelen ser los datos identificativos de la persona -nombre, apellidos, fecha y lugar de nacimiento, etc.- y algún número o código asociado que puede ser utilizado -mal utilizado- para el intercambio de información y cruce de datos no autorizado.

Este tratamiento de datos, con la posibilidad indicada de cesión[71] de los mismos a terceros o de utilización del resultado del tratamiento, atenta, en principio, contra una elemental protección a la intimidad de la persona y este es, en un primer aspecto, el derecho a proteger: el de la intimidad.

No podemos olvidar que los datos que tratamos en la empresa no son nuestros; son de sus titulares, de los interesados o afectados como los denomina la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

Es por ello que, cumpliendo con la normativa vigente, se pueden tratar los datos cuando ese tratamiento sea lícito pero teniendo en cuenta que estamos haciendo un tratamiento sobre datos que son de otros y que debemos respetar, consecuentemente, todos los principios y derechos que sobre ellos contempla la ley.

Es frecuente escuchar a responsables de empresas que dicen que tienen ficheros de datos suyos que les ha costado mucho tiempo conseguir. Tendrán ficheros de datos y será cierto que les habrá costado mucho tiempo conseguirlos, pero también es cierto que los datos no son suyos, son de sus titulares, y deberán ser tratados con la conciencia de que estamos trabajando sobre "algo que no es nuestro" y, por tanto, debe ser respetado, al menos en la forma que marca la licitud del tratamiento en las normas correspondientes.

Y esa forma de tratar los datos, que debe tener en consideración el titular del fichero, la empresa, se debe hacer considerando las tres fases en las que se estructura el tratamiento de datos de carácter personal y que es necesario su exposición para mejor comprender y aplicar la correspondiente normativa; interpretar las normas sobre protección de datos y fijar las obligaciones del titular del fichero se debe hacer teniendo en consideración los tres momentos o fases en que se desarrolla, o puede desarrollar, el tratamiento automatizado de datos de carácter personal y que son:

1. El momento de recabar los datos, bien sea directamente del interesado o de un tercero[72], en el que tiene gran importancia su licitud y lealtad[73], con las características de conocimiento y, en su caso, consentimiento del afectado;

2 El momento del tratamiento de los datos, que pueden ser cruzados y relacionados en forma automática junto con otros datos, buscando definir un perfil determinado del afectado que incluso él mismo llega a desconocer, y

3. El momento de la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento, conocida ésta última como "cesión o comunicación de datos", en la que, al igual que en la recogida y en el tratamiento, se tendrá que considerar el conocimiento y consentimiento del titular.

---

[70]Lo que representa un peligro, pues las facilidades de consulta y rapidez de acceso a la información permiten también la interconexión de bases de datos y la posibilidad de procesamiento, con una facilidad de cruce de los mismos y de localización de un perfil determinado, respecto a informaciones o modelos seleccionados.

[71]Definida en la letra i) del artículo 3 de la Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado".

[72]La vigente Ley de protección de datos (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, muestra con fuerza esta obligación de informar al afectado ya sea cuando los datos se recaben del propio interesado, que deberá ser informado en ese momento, o cuando se recaben de terceros, que deberá ser informado (art. 5.4), "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".

[73]El concepto de lealtad que al figurar en una ley puede parecer, y lo es, un concepto jurídico indeterminado, tiene gran importancia por la referencia expresa y concreta que a él hace la ley española de protección de datos y, con mayor fuerza, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE), publicada en el Diario Oficial, serie L, núm. 281, de 23 de noviembre.

Estos tres momentos deben estar siempre presentes en el estudio de los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que les permitan ejercer sus derechos.

2. NORMATIVA

La norma básica que debe conocer toda persona que trate datos de carácter personal es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En esta norma se reconoce a los ciudadanos unos derechos en el tratamiento de sus datos personales, estableciendo determinadas garantías que obligan a los titulares de ficheros[74] y, consecuentemente, nace la necesidad de realizar y establecer un entorno organizativo, con importantes repercusiones jurídicas, para cumplir con los principios contemplados en la norma y respetar el ejercicio de sus derechos por los ciudadanos.

Deben ser respetados los principios de protección de datos que se contemplan en la LOPD y organizar el flujo lógico de la información en la empresa de forma que sea fácil, y seguro, no solamente cumplir con lo establecido en la norma, sino también poder comprobar que se realiza el tratamiento lícito, adecuado, que permita poder atender todos los derechos de los ciudadanos titulares de datos.

Esta norma principal se acompaña de dos Reglamentos que, si bien no la desarrollan directamente a ella, porque corresponden a desarrollos referentes a su norma antecedente, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), permanecen vigentes en tanto en cuanto no la contradigan ni se produzca un desarrollo reglamentario posterior[75]. Y estos dos Reglamentos son el aprobado por 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, en adelante, Real Decreto 994/1999 o Reglamento de medidas de seguridad, y el Real Decreto 1332/1994, de 20 de junio que desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, en adelante, el Real Decreto 1332/1994 o el Reglamento.

3. ÓRGANO DE CONTROL

La Agencia Española de Protección de Datos (AEPD) es el órgano de control de la Protección de datos, tiene calidad de ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada y actúa con total independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Creada por la derogada LORTAD[76] y regulada en la vigente LOPD, la Agencia se muestra como la instancia a la que pueden acudir los afectados para ser tutelados en el ejercicio de sus derechos[77]. Existiendo actualmente, además de la Agencia Española de Protección de Datos, tres Agencias autonómicas, en Madrid, en Cataluña y en el País Vasco.

En el ejercicio de sus funciones públicas, y en defecto de lo que dispongan la LOPD y sus disposiciones de desarrollo, indica el apartado segundo, del artículo 35, de la LOPD, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

---

[74] A cualquier empresa que tenga o mantenga datos personales en un soporte automatizado o susceptible de tratamiento automatizado.

[75] Así se desprende de la Disposición Transitoria tercera de la LOPD.

[76] El apartado primero del artículo 34 de la LORTAD indicaba sobriamente "se crea la Agencia de Protección de Datos".

[77] Pero ello no quiere decir que deba presentarse como institución atemorizante dispuesta a sancionar e imponer fuertes multas a los titulares de los ficheros que, solamente por errores cometidos, aparezcan señalados por los afectados. Como órgano de control del cumplimiento de la ley deberá ejercer sus funciones al servicio de los ciudadanos y de la sociedad en su conjunto, cumpliendo sus fines de apoyo y desarrollo de una normativa, así como de cauce y ayuda interpretativa, pero no convirtiéndose en ese fiscalizador atemorizante, con exceso de poder, que impida, incluso, el desarrollo de elementos tecnológicos que podrían tener una función de servicio al desarrollo del hombre, situándonos, otra vez más, en posturas de retroceso o, al menos, de imposibilidad de desarrollo con los mismos parámetros que otros países de nuestro entorno socio-económico.

La Agencia la dirige el Director, quien ostenta también su representación, que será nombrado de entre quienes componen el Consejo Consultivo (art. 36) *"mediante Real Decreto, por un período de cuatro años",* teniendo la consideración de *"alto cargo".*

La Ley regula también el funcionamiento y las funciones de la Agencia y de su Director, entre las que señalamos, por ser de mayor interés en este trabajo, atender las peticiones y reclamaciones formuladas por las personas afectadas, proporcionar a las personas información acerca de sus derechos sobre esta materia, ejercer la potestad inspectora y la sancionadora en los términos previstos en la Ley, ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la Ley, ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos y, otras que tienden a velar por el cumplimiento de la legislación sobre protección de datos (art. 37) y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, cancelación y oposición.

Integrado en la Agencia, se encuentra el Registro General de Protección de Datos donde serán objeto de inscripción (art. 39), los ficheros de que sean titulares las Administraciones Públicas, cuando sea competente una Agencia de Protección de Datos autonómica, y los ficheros de titularidad privada.

Conviene destacar un ciclo de actuaciones administrativas que, en número de tres, configuran potestades, bien de la propia Agencia Española de Protección de Datos, bien de su Director, que distinguen y marcan claramente la línea operativa que en la práctica sirve como instrumento de control del cumplimiento de la Ley por el titular del fichero.

Nos referimos, en primer lugar, a la potestad inspectora, regulada en el artículo 40[78], que otorga a los funcionarios que ejerzan la inspección la consideración de autoridad pública en el desempeño de sus cometidos, facultándoles para solicitar la exhibición o el envío de documentos o de datos, así como para inspeccionar los equipos físicos y lógicos utilizados para el tratamiento accediendo a los locales donde se hallen instalados.

En segundo lugar, la LOPD otorga, al Director de la Agencia Española de Protección de Datos, potestad para inmovilizar los ficheros[79] en los casos en que el titular del mismo no atienda el requerimiento para cesar en la utilización o cesión ilícita de los datos.

Y, por último, la potestad sancionadora que, sin duda, constituye en la práctica el método más seguro para hacer cumplir a los reticentes y para una más eficaz protección de los derechos de los afectados. En la propia Exposición de Motivos de la derogada LORTAD se contemplaba la potestad sancionadora como lógico correlato de la función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, en cuyo caso procederá la oportuna responsabilidad disciplinaria, o sobre los privados, para cuyo supuesto se prevén sanciones pecuniarias.

En este sentido, entre las funciones de la Agencia Española de Protección de Datos, el apartado g) del artículo 37 de la Ley, contempla la de *"ejercer la potestad sancionadora en los términos previstos por el título VII de la presente Ley".*

4. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

El problema surge con el tratamiento del dato y las conclusiones que se puedan obtener al asociarle a una persona determinada; esta subjetivación y valoración es la que contiene una potencial agresividad al derecho fundamental de la persona.

---

[78]El primer apartado del artículo 40 de la LOPD indica que "Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos".

[79]Potestad que, bajo el epígrafe de "potestad de inmovilización de ficheros", se encuentra contemplada en el artículo 49 de la Ley.

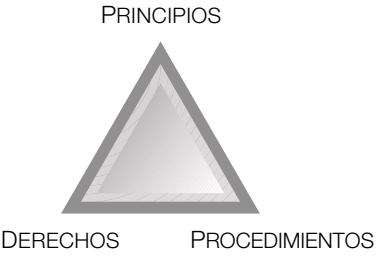
En principio, no se puede tratar ningún dato de carácter personal sin el consentimiento de su titular, interesado o afectado como le llama la Ley. Por tanto se podrán tratar todos aquellos datos para los que el titular de los mismos haya prestado su consentimiento salvo que concurra alguna excepción a esta necesidad de consentimiento como trataremos más adelante.

Es por tanto el titular de los datos el único que, como teoría general, puede decidir cuándo, dónde, cómo y por quién se tratan sus datos de carácter personal; y, además, con un derecho que ha sido elevado a la calidad de derecho fundamental.

Es así que, una vez conocidos qué datos se pueden tratar, pasaremos a ver en qué forma se deben tratar.

Los datos se deben tratar en la forma que queda especificada en la LOPD y que, resumida, consiste en contemplar los principios que figuran en el Título II[80] de la Ley y facilitar el ejercicio de los derechos de los ciudadanos mediante una adecuación de las normas de actuación en la empresa a lo que viene contemplado en el Título III[81] de la citada norma.

Esto es, no es suficiente contar con el consentimiento del titular del dato para poder proceder a su tratamiento, sino que, además, hay que adecuar ese tratamiento al respeto de los principios contemplados en la Ley y a facilitar el ejercicio de los derechos por el ciudadano.



Cabe estructurar el análisis y estudio de la protección de datos, siguiendo al Profesor Davara, como un triángulo en cuyos vértices se sitúan los principios de dicha protección, los derechos que emanan de dichos principios y los procedimientos que garantizan el ejercicio efectivo de dichos derechos. Es por ello que, de una forma práctica y orientada a esta adecuación de métodos y procedimientos en la empresa, pasamos a exponer los principios y derechos de la protección de datos.

5. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios, contemplados en el Título II de la LOPD, artículos 4 a 12, marcan las exigencias en el tratamiento de datos para que sea lícito en las tres fases que hemos mencionado. Los principios de la protección de datos deben ser considerados íntegramente tanto al recabar los datos, como al someterles a tratamiento, como al utilizar los resultados del tratamiento o, en su caso, comunicar o ceder los datos a terceros.

Lo mejor que se puede recomendar a una empresa cuando quiere saber cómo debe cumplir con la normativa sobre protección de datos, es decirle que analice el flujo lógico de la información en la entidad y compruebe que en los tres momentos o fases del tratamiento se cumplen los principios de la protección de datos contemplados en los artículos 4 a 12 de la LOPD, desde la propia calidad de los datos

[80] *El Título II de la LOPD, bajo el epígrafe principios de la protección de datos, establece los principios de: calidad de los datos (art. 4), información en la recogida de datos (art. 5), consentimiento (art. 6), datos especialmente protegidos (art. 7), datos relativos a la salud (art. 8), medidas de seguridad (art. 9), deber de secreto (art. 10), cesión o comunicación de datos (art. 11) y acceso a los datos por terceros (art. 12).*

[81] *El Título III de la LOPD, bajo el título derechos de las personas, contempla los derechos de: impugnación de valoraciones (art. 13), consulta al Registro General de Protección de Datos (art. 14), acceso (art. 15), rectificación y cancelación (art. 16) e indemnización (art. 19).*

hasta, en su caso, el acceso a datos por cuenta de terceros mediante la figura del encargado del tratamiento.

Es así como comenzaremos analizando los principios contemplados en la Ley; pero no lo vamos a hacer en el orden de los artículos de la norma sino en un orden lógico que permita en la práctica seguir con aprovechamiento su utilización e implementación; esto es, recomendamos seguir el orden lógico que exponemos para poder comprender de forma práctica cuáles son los principios y la forma de cumplirlos por el titular responsable del fichero o del tratamiento (la empresa).

Es así que empezamos por el denominado principio del consentimiento por considerarle, como ya hemos hecho referencia, el eje central de protección en nuestra norma.

a. El consentimiento del titular de los datos

La teoría general sobre la que gira nuestra norma de protección de datos es el llamado "principio del consentimiento" que podemos resumir, como ya hemos indicado, diciendo que el ciudadano es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior, o se dan a conocer sus datos a terceros; esto es, el afectado tiene que otorgar su consentimiento para que se pueda realizar un tratamiento de sus datos de carácter personal; dicho de otra forma, no se pueden tratar datos de carácter personal sin el consentimiento de su titular (del titular de los datos).

Pero, este principio general tiene sus excepciones. Veamos:

> *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*

indica el apartado primero del artículo 6 de la LOPD, pero, a continuación (apartado segundo), refiere una serie de casos en los que no es preciso el consentimiento para el tratamiento de los datos, exponiendo, vía excepción, que

> *"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".*

Analizando este apartado, y desde la óptica que nos ocupa en este trabajo[82], debemos señalar que las excepciones que aquí se contemplan a la exigencia del consentimiento son tres:

1. Cuando una ley así lo disponga.

2. Cuando los datos se recojan de fuentes accesibles al público[83]: en este caso que no haga falta consentimiento no quiere decir que no sea necesario el conocimiento y, por consiguiente, habrá que infor-

[82] *Se trata de un trabajo referido exclusivamente a ficheros cuyos titulares son las empresas, esto es, ficheros de titularidad privada. La LOPD hace una distinción contundente entre ficheros de titularidad pública y ficheros de titularidad privada, llegando incluso a dedicar dos capítulos diferentes (capítulo primero del Título IV, bajo la rúbrica de ficheros de titularidad pública y capítulo segundo del mismo Título IV, bajo la rúbrica de ficheros de titularidad privada), para separar características en su regulación; este trabajo se centra solamente en los ficheros de titularidad privada de las empresas e, independientemente de las críticas que nos merece esta clara diferenciación, centraremos la atención solamente sobre ellos.*

[83] *La letra j) del art. 3 de la LOPD define las fuentes accesibles al público como "aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes accesibles al público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación".*

mar al interesado en la forma que prescribe el artículo 5 de la LOPD sobre que se está realizando el tratamiento de sus datos y, naturalmente, el fichero, los datos recabados y el tratamiento que se efectúe, deberán ser adecuados a lo especificado en la norma.

3. Cuando los datos de carácter personal 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. Si entramos en el análisis de "la necesidad" exigida para el mantenimiento de las relaciones o para el cumplimiento del contrato, nos encontramos, como en todos los casos en que se manejan conceptos jurídicos indeterminados, con problemas de interpretación y, en particular, referente a esta cuestión, consideramos que debía existir, vía Instrucción, algún pronunciamiento de la Agencia Española de Protección de Datos.

En otro orden de cosas, podríamos expresar diversas teorías sobre si el consentimiento a que se refiere el artículo 6 de la LOPD, puede ser tácito y, en caso de que deba ser expreso, si debe ser por escrito.

Nuestra opinión es que el consentimiento, dependiendo de los casos de que se trate y la regulación que de él hace la Ley, puede ser en unos casos tácito, en otros expreso y, por último, para una categoría especial de datos, tiene que ser expreso y por escrito[84].

Señalar también que en el caso de que sea necesario el consentimiento, éste puede ser revocado; el apartado tercero del referido artículo 6, indica que:

> *"El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos".*

b. La calidad de los datos

Independientemente de lo que ya hemos expresado sobre la necesidad del consentimiento para recoger y tratar datos de carácter personal, y las excepciones al mismo, los datos que se recaben deben ser pertinentes y adecuados al fin que se pretenda, además de que no podrán permanecer en el fichero por tiempo mayor al necesario para cumplir con la finalidad para la que se obtuvieron.

La calidad de los datos, fuente de múltiples conflictos interpretativos, se encuentra reflejada en el artículo 4 de la LOPD que, con una amplia redacción en siete apartados, podemos resumir indicando que la información, o los datos que se recaban o que se registran en un fichero, debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales[85] y, añadimos nosotros, leales[86].

Ello exige, girando sobre el concepto de pertinencia de los datos, de acuerdo con el ámbito y la finalidad para los que se hayan obtenido, que vaya acompañado de su exactitud y su actualización[87].

La utilización de acuerdo con el fin para el que fueron obtenidos –adecuación al fin–, junto con la cancelación y sustitución de oficio en determinados supuestos –debido a su inexactitud total o parcial– y el almacenamiento de forma que el titular pueda ejercer su derecho de acceso, son los complementos que garantizan la calidad exigida por la norma.

---

[84]La LOPD al exigir el consentimiento lo hace de una forma genérica y, por lo tanto, cabe perfectamente el consentimiento tácito; cuando la Ley quiere que el consentimiento sea expreso lo declara con nitidez, llegando al extremo de exigir el consentimiento "expreso y por escrito" cuando se refiere al tratamiento de los datos que denomina "especialmente protegidos" y, en particular (apartado 2, del artículo 7), los que "revelen la ideología, afiliación sindical, religión y creencias". De igual forma, cuando se trata de "cesión de datos", se habla solamente de consentimiento sin exigencia de que sea expreso (así, apartado 1, del artículo 11). Que el consentimiento puede ser tácito se remacha también en el artículo 44 cuando al exponer los tipos de infracciones, indica (apartado 3) que son infracciones graves "c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible", con una agravación en la calificación de la infracción, (apartado 4) que califica de muy grave "c) Recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado".

[85]Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos, indica el séptimo apartado, del artículo 4 de la Ley.

[86]Los comentarios a la interpretación del término "lealtad" los realizamos en el apartado 7.b, y a ese lugar nos remitimos.

[87]Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, reza el tercer apartado del citado artículo 4 de la ley; pero, ¿qué debemos entender por puestos al día?; en muchas ocasiones, dificultades operativas y de gestión, incluso problemas de comunicación ajenos a nuestra voluntad, impiden la "puesta al día" de los datos.

De esta forma, a tenor de lo que establece la Ley, cuando los datos registrados sean inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, existiendo también la obligación de cancelarlos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

c. La información al recabar los datos

Es un principio general de protección de datos que todo ciudadano tiene derecho a conocer la información almacenada sobre sí mismo.

Cuando se recaben datos de una persona para ser utilizados mediante un tratamiento informático, o mantenerlos en un soporte susceptible de tratamiento automatizado, se debe realizar de una forma legal y leal; ello incluye que el afectado sea informado –de modo expreso, preciso e inequívoco, indica el primer apartado del artículo 5 de la LOPD–, de la finalidad de la recogida y de los destinatarios de la información, advirtiéndole si tiene o no obligación de contestar a las preguntas que se le realizan y de cuáles pueden ser las consecuencias en el caso de que se niegue a contestar o a proporcionar los datos.

Habrá que informarle también del derecho que tiene de ejercitar el acceso al fichero para saber los datos que de él se mantienen y, en su caso, exigir la rectificación o cancelación de los mismos cuando sean inexactos, obsoletos o no adecuados al fin perseguido. Asimismo, tendrá que indicarse la posibilidad de ejercitar el derecho de oposición[88] al tratamiento de datos, para aquellos casos en los que proceda. Como es natural, para que pueda ejercer sus derechos, se deberá notificar también al afectado sobre la identidad y dirección del responsable del fichero.

La LOPD distingue que los datos hayan sido recabados, o no, del propio interesado, señalando en el apartado cuarto, del artículo 5, que

> *"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*[89]*".*

d. Los llamados datos sensibles

La LOPD establece unas categorías de datos que deben ser objeto de especial protección[90]; es por ello que, en referencia directa al que hemos denominado principio del consentimiento, establece una excepción *sui generis* en el artículo 7.

El consentimiento del afectado, como ya hemos indicado, es necesario para recabar y tratar datos de carácter personal, "salvo que la ley disponga otra cosa"; pero este consentimiento puede ser tácito[91]; sin embargo, cuando se trata de los datos que el artículo 7 considera especialmente protegidos y a los que hacemos referencia, el consentimiento debe ser expreso, indicando, como mayor garantía, que en el caso de los datos a que se refiere el artículo 16.2. de la Constitución[92] y los datos referentes a la afiliación sindical, el consentimiento debe ser, además de expreso, por escrito.

---

[88] *El derecho de oposición es un derecho nuevo en la LOPD, como consecuencia de la transposición de la Directiva 95/46/CE, que no tiene desarrollo reglamentario aún y que se encuentra recogido en el artículo 6.4 de la LOPD, dedicado al consentimiento.*

[89] *Se refiere en concreto a la siguiente información, apartado primero del artículo 5 de la LOPD, "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"; "d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición", y "e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

[90] *En términos generales diremos que se trata de los datos referentes al origen racial, a la salud y a la vida sexual por un lado y, por otro lado, a la ideología, afiliación sindical, religión y creencias.*

[91] *Es necesario insistir en que, aun siendo válido el consentimiento tácito, acudiremos a él solamente en los casos en que sea absolutamente necesario, debido a las dificultades de prueba que tiene.*

[92] *Que son los que se refieren a la ideología, religión y creencias.*

Se completa la garantía sobre los datos que se refieran a la ideología, religión y creencias, y la exigencia de protección especial, al indicar el artículo que, además

> *"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".*
>
> *Al tiempo que se prohíbe la creación de ficheros 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.*

e. Las medidas de seguridad

El artículo 9 de la LOPD, desarrollado reglamentariamente por 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 (en adelante, como hemos indicado, Real Decreto 994/1999 o Reglamento de medidas de seguridad) establece que el responsable del fichero y, en su caso, el encargado del tratamiento deben adoptar las medidas de índole técnica y organizativas necesarias con el fin de garantizar la seguridad de los datos personales objeto de tratamiento, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Consiste en garantizar la confidencialidad e integridad de la información que se trata en los sistemas de información. En relación con la aplicación de las medidas de seguridad no vamos a extendernos más aquí remitiéndonos a un apartado posterior en el que se realiza un análisis exhaustivo de las mismas.

f. El deber de secreto

La LOPD, en su artículo 10, impone al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de datos la obligación de secreto profesional respecto de los datos tratados así como el deber de guardarlos, aún una vez finalizadas sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo. En relación con este deber de secreto nos remitimos al apartado de obligaciones del responsable del fichero en el que se desarrolla más ampliamente este principio.

g. La cesión o comunicación de datos

La cesión de datos es un punto conflictivo cuando se trata de proteger la llamada "privacidad"; de una parte, porque cediendo los datos a otros ficheros se posibilita el cruce de los mismos, aplicando con toda intensidad las posibilidades de tratamiento de la información que posee la informática y, de otra parte, porque la propia cesión facilita la utilización de los datos para un uso que no es el mismo para el que se habían recabado.

Respecto a la cesión de los datos, se detallan, en el artículo 11 de la Ley, las condiciones en las que podrán o no ser cedidos, indicando que no se podrán ceder los datos de carácter personal objeto de tratamiento automatizado más que:

> *"para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario"*

y, salvo que la Ley prevea otra cosa, o se trate de datos recogidos de fuentes accesibles al público, con el previo consentimiento del afectado o interesado.

Es, por tanto, necesario el consentimiento del afectado. Consentimiento que puede ser revocado y que será nulo cuando la información que se facilite al interesado no le permita conocer la finalidad a la que se destinarán los datos o el tipo de actividad de aquél a quien se pretenden comunicar; por tanto, se trata de un consentimiento específico para un cesionario también específico, determinando con claridad la finalidad de la cesión que se consiente.

No se indica que este consentimiento deberá ser escrito, ni revestir un formalismo determinado, de donde podemos deducir que puede ser tácito[93], siempre que podamos de él determinar con claridad la finalidad de la cesión que se consiente.

No será necesario el consentimiento, dice el apartado segundo del artículo 11:

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.

h. El encargado del tratamiento

Esta figura del encargado del tratamiento[94] que, por sí misma y en su definición, está recogida de una manera clara y diáfana, encuentra alto grado de complicación en la regulación que de su relación con el titular del fichero hace el artículo 12 de la Ley y que, sin duda, trae múltiples discusiones e interpretaciones en su adecuación práctica.

Termina el Título II de la LOPD, relativo a los principios de la protección de datos, con este artículo, que, como ya hemos referido, resulta polémico, en el que se establecen los requisitos para que el acceso a los datos por cuenta de terceros no sea considerado como comunicación o cesión, regulando la figura, ya citada, del "encargado del tratamiento".

Se indica en la norma que los tratamientos que se realicen por cuenta de terceros tendrán que figurar en un contrato que deberá constar por escrito *"o en cualquier otra forma que permita acreditar su celebración y contenido",* en el que se establecerán todas las características del tratamiento y se destacará expresamente que no se podrá comunicar estos datos, ni tan siquiera para su conservación, a terceros, con lo que queda totalmente prohibida la subcontratación.

La práctica y, expresado en otros términos, la necesidad y utilización real de esta figura, debe permitir el acceso a los datos, con una referencia en el contrato, y la consiguiente autorización por el titular del fichero, a aquellas personas a las que se podrá encargar un tratamiento específico; decimos, como aclaración, que, en nuestra opinión, si el titular del fichero autoriza en el contrato al que se refiere este artículo 12, a la contratación con un tercero determinado y específico, de unos también deter-

[93] *Para no provocar errores, insistimos en que el consentimiento tácito es válido siempre que la Ley no diga otra cosa (como es el caso de los datos especialmente protegidos), pero, volvemos a insistir, no es recomendable el consentimiento tácito por las dificultades de prueba que tiene. Hay que acudir al consentimiento tácito solamente en los casos en que sea absolutamente necesario.*

[94] *Al que en la letra g) del artículo 3 de la LOPD se le define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".*

minados y específicos tratamientos, estos no podrán ser considerados como subcontratación y tendrán cabida en la regulación de este artículo no tratándose, por tanto, de una comunicación o cesión.

6. DERECHOS DEL INTERESADO

Los principios se quedan en meras declaraciones teóricas si no tuvieran a su lado la posibilidad del ejercicio de unos derechos por el ciudadano que dieran contenido y efectividad práctica a esos principios.

De esta forma estamos obligados a decir que la empresa titular del fichero o del tratamiento no cumple solamente con tratar los datos de carácter personal respetando todos los principios recogidos en la norma sino que, además, es necesario que permita y facilite el ejercicio de los derechos por el interesado. Es decir, se debe estructurar un procedimiento lógico-administrativo que facilite el ejercicio de los derechos de acceso, rectificación, cancelación de los datos y oposición al tratamiento en la forma en que la LOPD contempla que pueden ser ejercidos y dentro de los plazos que figuran en la norma.

a. El derecho de impugnación de valoraciones

Nos referiremos en primer lugar al derecho de impugnación del interesado de determinados actos, cuando su fundamento sea un tratamiento automatizado de sus datos destinado a evaluar determinados aspectos de su personalidad, que se encuentra contemplado en el apartado segundo del artículo 13 de la norma que, bajo el epígrafe de "impugnación de valoraciones", expresa que:

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

Es difícil entender esa limitación del texto a su "único fundamento", ya que se puede suponer que si la valoración de su comportamiento ha sido producto de analizar en conjunto datos de carácter personal sometidos a un tratamiento automatizado, por ejemplo, y datos de carácter personal sometidos a un estudio manual[95], ya no es posible, de acuerdo con la redacción de este artículo, impugnar los actos a los que se refiere. Será sencillo, por tanto, fundamentar en forma mixta, mediante un tratamiento automatizado y otro no, para poder eludir la impugnación del acto. Un ejemplo en el que puede darse el ejercicio de este derecho es el de la concesión de una tarjeta de crédito, en la que previamente se analiza la situación financiera del solicitante.

b. El derecho de consulta al Registro General de Protección de Datos

No cabe duda de que uno de los derechos del afectado es ser informado en la recogida de datos y, naturalmente, se convierte en obligación del titular del fichero, o de la persona o entidad que recaba los datos, informarle de modo expreso, preciso e inequívoco, en la forma y con las características que ya hemos indicado.

Pero el derecho de consulta al Registro General de Protección de Datos contemplado en la Ley (artículo 14), es el del afectado a recabar del Registro General de Protección de Datos, la información tendente a conocer si existen y cuáles son los ficheros de datos de carácter personal, consulta que realizará tantas veces como tenga interés siendo el Registro General de Protección de Datos "de consulta pública y gratuita". Esta información puede obtenerse a través de la dirección en Internet de la Agencia Española de Protección de Datos (www.agpd.es).

[95] *Un estudio no sometido a operaciones técnicas, de acuerdo con la definición de tratamiento de datos que contempla el apartado c), del artículo 3, de la LOPD.*

c. El derecho de acceso

El afectado puede dirigirse al titular del fichero para conocer los datos que sobre él tiene registrados. Este es el sentido y fundamento del denominado "derecho de acceso".

En la práctica es mediante este derecho como el afectado obtiene, o debe obtener, una información exacta y veraz sobre sus datos de carácter personal que se encuentran en el fichero de nuestra empresa o, en su caso, información sobre que el fichero no contiene ningún dato de carácter personal sobre él mismo[96].

Este derecho puede ser ejercido por el ciudadano en intervalos no inferiores a doce meses, esto es, solamente lo podrá ejercer una vez cada doce meses, excepto que exista causa justificada (interés legítimo, dice la LOPD), que indique una periodicidad menor, o por la cual el afectado pueda ejercer en períodos de tiempo inferiores su derecho de acceso.

El ejercicio del derecho de acceso está contemplado en la LOPD y en el Reglamento que establece el procedimiento para llevarle a cabo; no obstante, la Instrucción 1/1998 de la Agencia Española de Protección de Datos[97] destaca algunas características vía interpretativa que debemos señalar:

1. El responsable del fichero tiene obligación de contestar a la solicitud del derecho de acceso aunque en el fichero no se encuentren, ni nunca se hayan encontrado, datos de la persona que solicita la información[98].

2. En la respuesta que se envíe al afectado como consecuencia del ejercicio de su derecho de acceso, se deberá emplear cualquier medio que acredite el envío y la recepción[99].

3. El responsable del fichero debe actuar diligentemente llegando incluso a tener una obligación de "hacer", consistente en apoyar al afectado para que pueda subsanar los defectos que tuviera su petición[100].

d. Los derechos de rectificación y de cancelación

El afectado, en el caso de que los datos sean inexactos, o cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido registrados, posee el derecho de rectificación o, en su caso, el derecho de cancelación; si los datos que se encuentran en un fichero son inexactos, incompletos o no existiera, por el motivo que fuera, derecho a su registro por parte del titular del fichero, el afectado podrá ejercer su derecho de rectificación o su derecho de cancelación[101].

El derecho a exigir que aquellos datos inexactos, incompletos o que hubieran dejado de ser pertinentes o adecuados para la finalidad para la que hubieran sido registrados, sean rectificados o cancelados se encuentra recogido en la Ley (art. 16) indicando que:

> *"El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días[102]".*

---

[96] *Indica el apartado primero del artículo 15 de la LOPD, que "el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".*

[97] *Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. Publicada en el Boletín Oficial del Estado núm. 25, de 29 de enero. Aunque debe entenderse derogada, por ser anterior a la LOPD, permite conocer el criterio interpretativo de la Agencia Española de Protección de Datos.*

[98] *El apartado cuarto de la norma primera de la Instrucción 1/1998, indica que "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, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción".*

[99] *No se entiende con facilidad qué se debe interpretar como acreditar la "recepción" ya que ésta no depende del responsable del fichero y, por tanto, si la persona que la debe recibir se niega a hacerlo será imposible acreditar dicha recepción; entendemos que lo que se quiere decir es que se pueda acreditar la recepción o el intento de entrega, aunque no se haya logrado que la reciba el afectado.*

[100] *El apartado cuarto, de la norma primera de la Instrucción 1/1998, en su último párrafo, indica que "el responsable del fichero deberá solicitar la subsanación" en el caso de que la solicitud no reúna los requisitos especificados en la propia Instrucción y, por lo tanto, no sea atendible.*

[101] *El apartado segundo del artículo 16 de la Ley, indica 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 y, en particular, cuando tales datos resulten inexactos o incompletos"*

[102] *Estos diez días han de entenderse y computarse, en el caso de los ficheros de titularidad privada, como días naturales, según la interpretación establecida por el Director de la Agencia Española de Protección de Datos con base en lo dispuesto en el apartado 2 del artículo 5 del Código Civil que dispone que "en el cómputo civil de los plazos no se excluyen los días inhábiles".*

Es así como los datos cuyo tratamiento no se ajuste a lo especificado en la Ley y, en particular, los datos que resulten ser inexactos o incompletos, serán rectificados o, en su caso, cancelados, debiendo comunicar el responsable del fichero esta circunstancia, con expresa indicación de los datos rectificados o cancelados, a todos aquellos a los que les hubiese cedido la información.

Cabe destacar que la cancelación no supone el borrado de los datos, sino su bloqueo; la figura del bloqueo, discutida y alarmantemente no entendida, por fin, tiene su respaldo en el propio texto de la norma.

La cancelación no puede exigir el borrado total y absoluto de los datos, aunque sea necesario el bloqueo con todas las características de seguridad que le deban acompañar; de otra forma, nos encontraríamos ante la extraña situación de que el borrado total de los datos no permitiría atender otras obligaciones, por no existir ya rastro alguno sobre los datos, como pueden ser los requerimientos realizados por los Jueces o Tribunales, o por la propia Administración, y teniendo en cuenta, además, que el responsable del fichero está obligado a atender las propias responsabilidades nacidas del tratamiento de los datos que exijan que no sean borrados, sino bloqueados, y cuya posibilidad ya queda recogida en el texto del artículo 16 de la LOPD[103].

Los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, indica el artículo 17 de la LOPD, se establecerán por vía reglamentaria; debemos hacer notar que permanecerán en vigor los procedimientos para el ejercicio de los derechos de acceso, rectificación y cancelación contemplados en el Reglamento que continua vigente[104].

Este procedimiento es de gran importancia, ya que establece, en la práctica, la efectividad de la Ley y el verdadero respeto –que no sólo reconocimiento– a los derechos en ella recogidos.

Ahora bien, es posible que la rectificación o, en su caso, la cancelación, no sea procedente y el responsable del fichero no esté, por tanto, obligado a realizarla; en este caso pondrá en conocimiento del afectado, en el mismo plazo de diez días, la no procedencia de la rectificación o la cancelación solicitada argumentando los motivos por los que no la realiza[105].

Si pasados los diez días, el afectado no recibe respuesta alguna a su solicitud de rectificación o de cancelación, a efectos de interponer la reclamación que corresponda, se entenderá que la solicitud ha sido desestimada.

En el caso del ejercicio de los derechos de rectificación y cancelación la Instrucción 1/1998 también destaca algunas características vía interpretativa que debemos señalar:

1. La solicitud de rectificación que haga el afectado deberá señalar el dato que se considera erróneo y la corrección que se debe realizar, así como acompañar la documentación que lo justifique.

2. Si el responsable del fichero hubiera cedido a un tercero los datos que hayan sido rectificados o cancelados se le deberá comunicar que se ha efectuado la rectificación o cancelación y en qué ha consistido para que él (el tercero cesionario de los datos), actúe en consecuencia.

3. Indica el apartado cuarto de la norma tercera de la Instrucción que estamos comentando que *en la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda,* cuestión a tener en cuenta y que creemos no necesita más comentario.

---

[103] El artículo 16 de la LOPD indica, en su tercer apartado, que "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".

[104] Artículos 12 y ss. del Real Decreto 1332/1994.

[105] "En el supuesto de que el responsable del fichero considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente y dentro del plazo señalado en el apartado anterior, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992", indica el apartado tercero, del artículo 15 del Reglamento.

4. Por último, señalar que la solicitud de rectificación o cancelación no resulta de obligado cumplimiento por el responsable del fichero, sino que solamente debe atender la petición pero no está obligado a llevar a cabo la rectificación o la cancelación cuando no sean procedentes.

Conviene reseñar que la normativa señala unos requisitos generales para el ejercicio de los derechos de acceso, rectificación y cancelación [106] entre los que destaca su carácter de personalísimos, pudiendo solamente ser ejercidos por el afectado y ante el responsable del fichero; no es válido, por tanto, el ejercicio de los derechos mediante representante a excepción, cuestión lógica, de aquellas personas que se encuentren en situación de incapacidad jurídica o sean menores de edad, que les imposibilita el ejercicio personal de los derechos y que podrán realizarlo a través de su representante que deberá acreditar ante el titular del fichero su representación.

Llama extraordinariamente la atención que la Instrucción 1/1998, también con carácter general para los derechos de acceso, rectificación y cancelación, indica que todas las personas de la organización del responsable del fichero que tengan acceso a datos de carácter personal [107] deben estar preparadas para poder informar al afectado del procedimiento a seguir para el ejercicio de sus derechos, lo que implica que el responsable del fichero debe tomar las medidas oportunas para garantizarlo.

Añadir que, respecto a los requisitos generales de los tres derechos que nos ocupan, indican, tanto la Ley, como el Reglamento y la Instrucción 1/1998, características operativas que en algunos casos se repiten hasta la saciedad, no presentando ningún aspecto de aclaración, sino que incluso dejan pensar que fueron incluidas de relleno para dar más consistencia o, apariencia al texto; no obstante, sí conviene citar que:

– Los derechos de acceso, rectificación y cancelación son derechos independientes, en el sentido de que no se puede exigir el ejercicio previo de uno de ellos para ejercer otro cualquiera.

– Se deberán ejercer mediante solicitud dirigida al responsable del fichero conteniendo la identificación del afectado [108], la petición que solicita, el domicilio a efectos de notificaciones y los documentos acreditativos que, en su caso, sean necesarios para apoyar la petición que formula.

e. El derecho de oposición

Como ya hemos indicado, la LOPD introduce un nuevo derecho, el derecho de oposición, a raíz de la transposición de la Directiva. Este derecho carece de desarrollo reglamentario, y se encuentra recogido dentro del título dedicado a los principios, concretamente en el artículo 6 destinado al consentimiento, que dice así:

> *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.*

No obstante hay que tener en cuenta que este derecho, de un lado, como deciamos, no tiene desarrollo reglamentario que especifique su ejercicio, y de otro, la AEPD está interpretando que su ejercicio debe ser conforme con el del derecho de acceso.

---

[106] Además, la LOPD ha añadido el derecho de oposición, pero dicho derecho, por un lado, no se encuentra claramente definido (no hay más que llamar la atención, por ejemplo, sobre su ubicación en el artículo 6.4 dentro del principio del consentimiento) y tampoco está desarrollado reglamentariamente, por lo que no es posible establecer un procedimiento para un derecho sólo enumerado.

[107] Expresión que tiene un contenido muy amplio pues acceso a datos de carácter personal en un sistema automatizado pueden tener múltiples personas, desde los operadores del sistema, programadores, analistas y cualquier otro personal informático; no parece operativo que el afectado pueda dirigirse a cualquiera de estas personas y haya que estructurar una estrategia para poder cumplir con lo indicado en la Instrucción, con la consiguiente inseguridad que para el propio afectado podría esto llevar consigo.

[108] Identificación que la Instrucción 1/1998 centra como válida con la "fotocopia del documento nacional de identidad del afectado", aunque, bien es cierto que podrá ser sustituida siempre "que se acredite la identidad por cualquier otro medio válido en derecho" (segundo párrafo, del apartado tercero, de la norma segunda).

A continuación se presenta una tabla que posibilita la rápida comprensión de los derechos analizados.

TABLA I: DERECHOS DEL INTERESADO

Derecho de impugnación de valoraciones	El derecho de impugnación de valoraciones consiste en: • la facultad del interesado, • de no verse sometido a una decisión con efectos jurídicos, • que le afecte de manera significativa, • efectuada sobre la base de un tratamiento de datos, • destinado a evaluar determinados aspectos de su personalidad.
Derecho de acceso al RGPD	Mediante el ejercicio de este derecho: • cualquier persona podrá recabar información, • ante el Registro General de Protección de Datos (RGPD), • sobre: – la existencia de tratamientos de datos, – o sus finalidades, y – la identidad del responsable del tratamiento • de forma gratuita.
Derecho de acceso	Consiste en la facultad del interesado para: • solicitar, y • obtener información sobre: – sus datos sometidos a tratamiento, – el origen de los mismos, y – las comunicaciones realizadas o que se prevean realizar • de forma gratuita Ejercitándose a intervalos no inferiores a 12 meses, salvo que se acredite un interés legítimo.
Derechos de rectificación y cancelación	Supone la facultad del interesado de: • instar al responsable del fichero a: – rectificar o cancelar, – los datos cuyo tratamiento no se ajuste a la Ley y, en particular, – resulten inexactos o incompletos • en el plazo de diez días.
Derecho de oposición	Consiste en la facultad del interesado para: • oponerse al tratamiento de sus datos, • cuando no sea necesario su consentimiento para el tratamiento, • existan motivos fundados y legítimos para ello, y • una ley no disponga lo contrario.
Características de los derechos	Los derechos de acceso, rectificación y cancelación se caracterizan por ser: • personalísimos, • si bien cabe la actuación del representante legal cuando el interesado se encuentre en situación de: – incapacidad, o – minoría de edad – o que le imposibilite para el ejercicio personal de los mismos • son derechos independientes.
Ejercicio	Los derechos conferidos al interesado: • serán ejercidos ante el responsable del fichero, • mediante solicitud dirigida al mismo con el contenido legalmente determinado, • el ejercicio de uno no es requisito previo para el ejercicio de otro derecho.

7. OBLIGACIONES DEL RESPONSABLE DEL FICHERO

En general, podríamos decir que las obligaciones del responsable del fichero se centran en tomar todas las medidas necesarias orientadas a impedir el abuso o mal empleo de la información, así como hacer un tratamiento de los datos legal y leal; pero no terminan ahí las obligaciones ya que se completan, en ambas direcciones, de forma que el afectado pueda tener conocimiento exacto y real de la situación de sus datos en el fichero, al tiempo que se le facilite el ejercicio de sus derechos.

Así, destacando alguna de las obligaciones más significativas del titular del fichero, diremos que toda persona [109] que mantenga un archivo con datos de carácter personal, está obligada a:

a. Inscribirlo en el Registro General de Protección de Datos

Toda institución, pública o privada, que posea un fichero de datos de carácter personal, tiene la obligación de comunicarlo a la Agencia Española de Protección de Datos que, tras el análisis de su contenido y si cumple con todos los requisitos exigidos por la propia LOPD y por el Reglamento, lo inscribirá en el Registro General de Protección de Datos. También deberán notificarse a la Agencia los cambios que se produzcan *en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.*

No obstante, este análisis no implica un control a priori del cumplimiento de la LOPD ni tampoco supone que el fichero cumpla con estos requisitos en el sentido de que el tratamiento sea legal. Es solamente un trámite administrativo que permite al responsable del fichero o tratamiento cumplir con una de las obligaciones que le impone la normativa sobre protección de datos, si bien el Registro General de Protección de Datos comprueba que la inscripción efectuada cumple con los requisitos exigidos para dicha notificación.

Para realizar estas comunicaciones, la propia Agencia Española de Protección de Datos ha elaborado unos impresos o formularios [110], que facilitan al titular del fichero exponer los requisitos que son exigidos por la Ley y por el Reglamento, entre los que se encuentran la identificación del responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar.

b. Tratamiento legal y leal

En este apartado debemos recordar los tres momentos en los que hemos indicado que se configura el tratamiento de datos: 1.- Cuando se recaba el dato. 2.- Cuando se procede al tratamiento. 3.- Cuando el dato es utilizado o cedido; el tratamiento legal y leal debe realizarse en todas las fases, respetando los derechos del afectado y ciñendo el tratamiento a los principios establecidos en la norma.

La inscripción del fichero es solamente la primera obligación pero, al ser "vivo" el tratamiento de los datos (altas, bajas, modificaciones), su utilización y, en su caso, cesión, exigen se haga en forma legal y leal.

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.

---

[109] Tanto física como jurídica, con o sin ánimo de lucro. Solamente no se encuentran bajo el ámbito de aplicación de la Ley, de acuerdo con lo especificado en el apartado tercero del artículo 2, "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."

[110] Resolución de 30 de mayo de 2000, de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos, publicada en el Boletín Oficial del Estado núm. 153, de 27 de junio. Disponibles en www.agpd.es.

El principio de la lealtad –tanto al recabar los datos, con un conocimiento consciente e informado, como en el tratamiento y en la utilización o cesión posterior–, que tantas veces es discutido y malinterpretado y que no puede servir para encubrir fines diferentes a los que realmente pretende proteger, puede ser, y en muchas ocasiones lo es, punto controvertido en el estudio del tratamiento de datos de carácter personal.

c. Facilitar el ejercicio de los derechos

El titular del fichero tiene la obligación de facilitar, con diligencia, el ejercicio de los derechos al afectado de forma que sea una ayuda que permita la máxima transparencia, y la lealtad en el tratamiento de la que ya hemos hablado; hasta tal punto esto es así que, como hemos dicho, la Instrucción 1/1998 indica que 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.

Los plazos en los que se debe hacer efectivo el derecho de rectificación o el de cancelación ejercido por el afectado (diez días[111]), muestran con claridad el interés del legislador en que el titular del dato se encuentre con la atención precisa y rápida por parte del responsable del fichero.

Incluso la obligación de facilitar el ejercicio de los derechos al ciudadano, se lleva al extremo de que la Instrucción 1/1998, obliga al responsable del fichero a solicitar al afectado la subsanación de los defectos que pueda tener su solicitud cuando ésta no reúna los requisitos que exige la norma.

d. Deber de secreto

El responsable del fichero, indica el artículo 10 de la LOPD, y quienes intervengan en cualquier fase del tratatamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Ello implica que, en la práctica, las personas que deban operar sobre los ficheros tienen que estar bajo normas severas de conducta para el mantenimiento del secreto y para poder prevenir el mal uso de los datos.

Es natural esta exigencia si se tiene en cuenta el carácter que el legislador quiere imprimir a los datos de carácter personal cuando son susceptibles de tratamiento, llevando las consecuencias hasta los extremos que se consideren necesarios para garantizar el respeto a la intimidad y, como reza el artículo 18.4 de la Constitución, "el honor personal y familiar".

e. Medidas de seguridad

La seguridad debe ser extremada al máximo para impedir el acceso a los ficheros, en particular, y a los datos en general, a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos; pero la seguridad debe ser también tenida en cuenta para garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del afectado.

A la seguridad dedica la LOPD, el artículo 9, indicando que:

> *"El responsable del fichero y, en su caso, el encargado del tratamiento 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".*

[111] *Estos diez días han de entenderse y computarse, en el caso de los ficheros de titularidad privada, como días naturales, según la interpretación establecida por el Director de la Agencia Española de Protección de Datos con base en lo dispuesto en el apartado 2 del artículo 5 del Código Civil que dispone que "en el cómputo civil de los plazos no se excluyen los días inhábiles".*

artículo que ha sido desarrollado mediante el Real Decreto 994/1999, de 11 de junio, ya citado, que establece unas obligaciones para el titular del fichero, orientadas a la adopción de medidas de índole técnica y organizativas para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos.

Este Real Decreto por el que se aprueba el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal, contempla tres niveles de medidas de seguridad -nivel básico, nivel medio y nivel alto- que 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. Existe también un tipo de ficheros, los que permiten obtener una evaluación de la personalidad del individuo, que tienen que cumplir, además de las medidas de nivel básico, algunas de las de nivel medio, en concreto, las contenidas en los artículos 17 a 20 del Reglamento, por lo que puede hablarse, aunque no en términos estrictos normativamente hablando, de un "nivel intermedio".

e.1. Medidas de seguridad de nivel básico

El nivel básico se aplicará a todos los ficheros que contengan datos de carácter personal y comprende:

a) La creación por el responsable del fichero de un documento de seguridad de obligado cumplimiento para el personal que tenga acceso a los datos y a los sistemas de información y que contendrá las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido, las funciones y obligaciones del personal, la estructura de los ficheros con datos de carácter personal, el procedimiento de notificación, gestión y respuesta de las incidencias, entendiendo por incidencias, cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos y, por último, los procedimientos de realización de copias de respaldo y de recuperación de los datos,

b) La adopción por el responsable del fichero de 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,

c) La creación de un registro de incidencias en el sentido ya expuesto como tales,

d) La creación de una relación actualizada de usuarios (entendiendo por tales -por usuarios- los sujetos o procesos autorizados para acceder a los datos o recursos), que tengan acceso al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso,

e) El establecimiento de un mecanismo de control de acceso y

f) El establecimiento de un mecanismo de control de soportes.

e.2. Medidas de seguridad de nivel medio

El nivel medio se aplicará a los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito; estos ficheros que son clasificados como de "nivel medio", deberán reunir, además de las medidas de nivel básico que ya hemos referido, las siguientes referentes a que el documento de seguridad deberá contemplar todas las características citadas para los ficheros de nivel básico y además contendrá la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Destacaremos para los ficheros que deben cumplir las medidas de nivel medio que los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa que verifique el cumplimiento del propio Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

Completa las exigencias para este tipo de ficheros el establecimiento de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema y la verificación de que está autorizado, limitándose la posibilidad de intentar reiteradamente el acceso no autorizado, junto con otras limitaciones, en este caso de acceso físico a los locales donde se encuentren ubicados los sistemas de información, permitiéndolo solamente a aquellas personas autorizadas.

Por último, se establecen normas para la gestión de soportes, procedimientos de recuperación de datos y pruebas con datos reales que no estarán permitidas salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

e.3. Medidas de seguridad de nivel alto

El nivel alto se aplicará a los ficheros que contengan datos de los que denomina la LOPD especialmente protegidos [112], así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.

Estos ficheros deberán reunir, además de las medidas establecidas para los de nivel básico y las establecidas para los de nivel medio, otras medidas complementarias relativas a la distribución de soportes, al registro de accesos, a las copias de respaldo y recuperación y, en caso de que se realice transmisión de datos a través de redes de telecomunicaciones, se exige el cifrado de los mismos.

Vemos, por tanto, que no se trata solamente de cumplir una normativa sobre protección de datos en la forma que estamos indicando, sino también de establecer unas medidas de seguridad mínimas, exigibles a todos los titulares de ficheros, que garanticen la propia seguridad e integridad de la información cuando se trata de utilización de datos de carácter personal.

Es el titular del fichero quien debe adoptar, y, por tanto, será responsable de ello, de acuerdo con lo que especifica el apartado primero del artículo 9 de la LOPD, *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.*

Dado el enorme interés y consecuencias prácticas que la adopción e implementación de las medidas de seguridad tienen para la empresa, hemos considerado, en aras a proporcionar la mayor utilidad para el gestor, necesario y sumamente conveniente exponer las medidas de seguridad en una tabla analítica.

[112] *A los que ya nos hemos referido anteriormente y que son los relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y a la comisión de infracciones penales o administrativas.*

TABLA II. MEDIDAS DE SEGURIDAD

Documento de Seguridad (arts. 8 y 15)	Existencia de una normativa de seguridad descrita en un documento de obligado cumplimiento para todo el personal con acceso a los ficheros. Contenido del Documento de Seguridad: • Ámbito de aplicación con especificación detallada de los recursos protegidos • Medidas, normas, procedimientos y estándares • Funciones y obligaciones del personal • Estructura de los ficheros de datos y los sistemas de información que los tratan • Procedimientos de notificación, gestión y respuesta ante las incidencias • Procedimiento de actualización de los últimos cambios producidos en la aplicación o en la organización • Adecuación a las últimas disposiciones vigentes en materia de seguridad de datos • Identificación del responsable de seguridad • Controles periódicos para verificar lo dispuesto en el documento de seguridad • Medidas a adoptar para el desechado o reutilización de soportes
Funciones y obligaciones del personal (art. 9)	Las funciones y obligaciones de cada una de las personas con acceso a: • Los datos de carácter personal • Los sistemas de información estarán claramente definidas y documentadas El responsable del fichero adoptará las medidas necesarias para que el personal conozca: • Las normas de seguridad que afectan al desarrollo de sus funciones • Las consecuencias en que pudiera incurrir en caso de incumplimiento
Responsable de Seguridad (art. 16)	Designación de uno varios responsables de seguridad por el responsable del fichero para coordinar y controlar las medidas definidas en el Documento de Seguridad
Registro de incidencias (arts. 10 y 21)	Constará: • El tipo de incidencia • El momento en que se ha producido • Persona que lo notifica • A quién se lo comunica • Los efectos derivados de la misma Procedimientos realizados de recuperación de datos, persona que ejecutó el proceso, datos restaurados y los datos que han sido necesarios grabar manualmente. Necesidad de autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de datos.
Identificación y autenticación (arts. 11 y 18)	Existencia de una relación actualizada de usuarios con acceso autorizado al sistema de información y procedimientos de identificación y autenticación para dicho acceso. Procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad de las contraseñas empleadas como mecanismo de autenticación. Periodicidad del cambio de contraseñas y almacenamiento de forma ininteligible mientras estén vigentes. Mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario que intente acceder al sistema de información y la verificación de que está autorizado. Limitación de la posibilidad de intentar reiteradamente el acceso no autorizado al sistema.

TABLA II. MEDIDAS DE SEGURIDAD (Continuación)

Control de acceso (art. 12)	Los usuarios únicamente tendrán acceso a los datos o recursos que precisen para el desarrollo de sus funciones. El responsable del fichero establecerá los mecanismos para evitar el acceso a datos o recursos con derechos distintos a los autorizados. La relación de usuarios con acceso al sistema de información contendrá el acceso autorizado para cada uno de ellos. Exclusivamente el personal autorizado en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado conforme a los criterios establecidos por el responsable del fichero.
Control de acceso físico (art. 19)	Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información.
Gestión de soportes (arts. 13 y 20)	Los soportes informáticos que contengan datos deberán: • Permitir identificar el tipo de información que contienen • Ser inventariados • Almacenarse en un lugar con acceso restringido al personal autorizado para ello en el Documento de Seguridad La salida fuera de los locales en los que esté ubicado el fichero únicamente podrá ser autorizada por el responsable del fichero. El sistema de registro de entrada deberá permitir, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de recepción que deberá estar debidamente autorizada. El sistema de registro de salida permitirá, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada. En caso de desecho o reutilización de soportes se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario. En caso de operaciones de mantenimiento fuera de los locales en que se encuentren ubicados los ficheros, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.
Copias de respaldo y recuperación (arts. 14 y 25)	El responsable del fichero verificará la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación. Los procedimientos establecidos deberán garantizar la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se haya producido ninguna actualización de los datos. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de datos en un lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan, que deberá cumplir las medidas de seguridad exigidas.
Auditoría (art. 17)	Externa o interna de los sistemas de información e instalaciones de tratamiento, que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad, al menos, cada dos años.

TABLA II. MEDIDAS DE SEGURIDAD (Continuación)

Auditoría (art. 17)	El informe de auditoría dictaminará sobre la adecuación de las medidas y controles al Reglamento, identificando las deficiencias y proponiendo las medidas correctoras o complementarias necesarias. Incluirá 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, 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.
Pruebas con datos reales (art. 22)	Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
Registro de accesos (art. 24)	Como mínimo, se guardará de cada acceso 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. Si el acceso ha sido autorizado, se guardará la información que permita identificar el registro accedido. Los mecanismos que permiten el registro de los datos anteriores estarán bajo el control del responsable de seguridad sin que se deba permitir su desactivación. Los datos registrados se conservarán durante un período mínimo de dos años. El responsable de seguridad revisará periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.
Distribución de soportes (art. 23)	Se realizará cifrando los datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.
Telecomunicaciones (art. 26)	La transmisión de datos a través de redes de telecomunicaciones se hará mediante su cifrado o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

A continuación recogemos un checklist de comprobación de las medidas de seguridad, cuya utilidad consideramos máxima pues sirve, de un lado, para comprobar la implantación de las mismas en la entidad y, de otro, para adoptarlas, en caso de que aún no se haya hecho. Con el fin de proporcionar una herramienta lo más completa posible, hemos incluido el checklist que se utilizaría para un fichero de nivel alto, pues, como las obligaciones son acumulativas, se tiene asimismo que cumplir las medidas de nivel básico y medio. Para diferenciar el nivel al que pertenece cada medida se ha añadido entre paréntesis una indicación: B (básico), M (medio) y A (alto).

TABLA III: CHECKLIST DE MEDIDAS DE SEGURIDAD DE NIVEL ALTO

CONCEPTO	CUMPLIMIENTO PRÁCTICO
Tipos de ficheros (B)	
Estructura de los ficheros (B)	
Tipos de programas (B)	
Tipos de soportes (B)	
Sistema de registro de entrada de soportes informáticos: (M) Tipo de soporte Fecha y hora Emisor Número de soportes Tipo de información contenida Forma de envío Responsable autorizado recepción	
Sistema de registro de salida de soportes informáticos: (M) Tipo de soporte Fecha y hora Destinatario Número de soportes Tipo de información contenida Forma de envío Responsable autorizado recepción	
Soportes reutilizados (M) Medidas de control Imposibilidad recuperar información	
Soportes desechados (M) Medidas de control Imposibilidad recuperar información	
Distribución de soportes con información (A) Garantía inteligibilidad Garantía de no manipulación	
Tipos de equipos (B)	
Sistemas de información (B)	
Transmisión de datos por redes de telecomunicaciones (A) Garantía inteligibilidad Garantía de no manipulación	
Procedimientos de identificación (B)	
Procedimientos de autenticación (B)	

TABLA III: CHECKLIST DE MEDIDAS DE SEGURIDAD DE NIVEL ALTO (continuación)

CONCEPTO	CUMPLIMIENTO PRÁCTICO
Si contraseñas (B) Asignación Distribución Almacenamiento Garantía de confidencialidad Garantía de integridad Periodicidad en el cambio Almacenamiento ininteligible	
Relación actualizada usuarios con acceso autorizado (B) Sujetos Procesos	
Acceso autorizado (B) Según usuario Según funciones	
Criterios de (B) Concesión Alteración Anulación Del acceso autorizado	
Quién puede Conceder Alterar Anular el acceso autorizado	
Verificación autorización acceso (M) Registro de accesos (A) Identificación usuario Fecha y hora Fichero accedido Tipo de acceso Autorización de acceso Identificación registro accedido Denegación de acceso Conservación 2 años datos registrados	
Mecanismos registros de accesos (A)	
Revisión información registros de accesos (A)	
Informe mensual revisiones realizadas (A)	
Informe mensual problemas detectados (A)	
Personal autorizado en locales de ubicación del sistema (M) Control de acceso físico	
Ejecución tratamiento fuera de locales (B) Autorización escrita responsable fichero	

TABLA III: CHECKLIST DE MEDIDAS DE SEGURIDAD DE NIVEL ALTO (continuación)

CONCEPTO	CUMPLIMIENTO PRÁCTICO
Funciones del personal (B)	
Documentación funciones del personal (B)	
Responsable de seguridad (M) Coordinación/control medidas Conclusiones informe auditoría	
Procedimiento notificación incidencias (B)	
Procedimiento gestión incidencias (B)	
Procedimiento respuesta incidencias (B)	
Registro de incidencias (B) Tipo de incidencia Momento de su producción Persona que la notifica Persona a la que se comunica Efectos de la incidencia Procedimientos recuperación datos (M) Persona ejecuta proceso Datos restaurados Datos grabados manualmente en la recuperación	
Auditoría externa o interna cada dos años mínimo (M)	
Informe de auditoría (M) Adecuación medidas Adecuación controles Identificación deficiencias Propuesta medidas correctoras Documentación conclusiones Datos Hechos Observaciones	
Medidas correctoras adoptadas según informe de auditoría (M)	
Copias de respaldo (B) Periodicidad semanal mínima (salvo no alteración) Conservación en lugar distinto al de ubicación equipos (A)	
Copias de recuperación (B) Procedimientos Conservación copia en lugar distinto al de ubicación equipos (A) Aplicación Garantía reconstrucción íntegra	
Autorización por escrito de procedimientos recuperación de datos (M)	
Actualización del documento (B)	
Revisión documento por cambios relevantes en sistema de información (B)	
Adecuación del documento (B)	

8. PROCEDIMIENTOS

El ciclo del tratamiento de los datos y de su protección correspondiente en defensa del derecho fundamental que hemos expuesto, se concluye con los denominados procedimientos.

Aunque haya que respetar por la empresa titular del fichero los principios de la protección de datos contemplados en la norma y que hemos expuesto; aunque la empresa ponga todos los medios para que el interesado pueda ejercer sus derechos y sea atendido en los plazos indicados, aunque se den todas estas cosas, deben existir unos procedimientos mediante los cuales el ciudadano pueda verse tutelado en el caso de que considere que no se está produciendo un tratamiento de datos legal.

A estos procedimientos dedicamos nuestra atención de una forma específica por la importancia que tienen para completar un tratamiento de datos en nuestra entidad que sea, como ya hemos indicado varias veces, legal y leal.

a. Procedimiento de inscripción de ficheros

Una empresa puede tomar la decisión de crear un fichero de datos de carácter personal cuando lo considere conveniente para sus intereses y desarrollo de su objeto social.

Ahora bien, una vez tomada esta decisión hay que proceder a inscribir ese fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Los artículos 25 a 30 de la LOPD, regulan –respecto a los ficheros de titularidad privada–, la creación, notificándolo previamente a la Agencia Española de Protección de Datos (art. 26.1), remitiendo a posterior desarrollo reglamentario [113] respecto al contenido de esta notificación que, no obstante, se exige que necesariamente figure (art. 26.2)

> *"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".*

Tras esta comunicación, y si se ajusta y cumple con todos los requisitos, el fichero se inscribirá en el Registro General de Protección de Datos (art. 26.4).

En el Real Decreto 1332/1994 [114] figura el procedimiento para la notificación e inscripción de ficheros y a ese lugar nos remitimos; no obstante, conviene decir que la Agencia Española de Protección de Datos ha elaborado unos impresos para la inscripción, modificación y supresión o baja de ficheros y recomienda, además, que la inscripción se realice a través de Internet [113].

b. Procedimiento de acceso

El procedimiento de acceso, que la LOPD indica, será establecido reglamentariamente [116], se encuentra regulado en el Reglamento (artículos 12 a 16) y "aclarado" [117] en la Instrucción 1/1998, exponiendo tanto las características y requisitos que debe contener el ejercicio de los derechos para que puedan hacerse efectivos, como el contenido de la información que el titular del fichero debe proporcionar al afectado cuando éste la solicite.

---

[113] Desarrollado mediante el Real Decreto 1332/1994, citado.

[114] En el capítulo III, artículos 6 a 8, del Real Decreto 1332/1994, figura el procedimiento de notificación de los ficheros de titularidad privada y el de inscripción de los mismos; repetir en este lugar esos artículos no nos ha parecido adecuado.

[115] Resolución de 30 de mayo de 2000, ya citada anteriormente.

[116] Primer apartado del artículo 17 de la LOPD.

[117] Según expresión literal de la introducción de la Instrucción 1/1998 al indicar que "esta Instrucción tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación", aunque nosotros creemos que lo que realmente hace es mostrar la interpretación que la Agencia Española de Protección de Datos da a la LOPD y al Reglamento, respecto al ejercicio por el afectado de los citados derechos.

Cabe destacar que la Instrucción 1/1998 incluyó alguna novedad significativa tanto en la solicitud, por el afectado, del derecho, como en la respuesta que le debe dar el titular del fichero. Señalamos, por ejemplo, la obligación, en ambos casos, del afectado y del titular o responsable del fichero, de acreditar el envío y la recepción de la solicitud en el caso del afectado[118], como el envío y la recepción de la respuesta en el caso del responsable del fichero.

La forma de ejercer los derechos, en la práctica, mediante solicitud dirigida al responsable del fichero, queda clara tanto en la redacción que da el Reglamento como en la, casi idéntica, que da la Instrucción 1/1998 y que se plasma en el apartado tercero, de la norma primera, de la Instrucción, que indica:

> *El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:*
>
> *Nombre, apellidos del interesado y fotocopia del documento nacional de identidad del interesado y en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.*
>
> *Petición en que se concreta la solicitud.*
>
> *Domicilio a efectos de notificaciones, fecha y firma del solicitante.*
>
> *Documentos acreditativos de la petición que formula, en su caso.*

Indicando también que, al ejercitar el derecho de acceso, el afectado podrá optar por:

> *Uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:*
>
> *a) Visualización en pantalla*
>
> *b) Escrito, copia o fotocopia remitida por correo*
>
> *c) Telecopia*
>
> *d) Cualquier otro procedimiento que sea adecuado a la configuración o implantación material del fichero, ofrecido por el responsable del mismo*

El responsable del fichero debe contestar a la indicada solicitud tanto si en el fichero figuran datos del afectado que ha realizado la solicitud, como si no figura ningún dato sobre dicha persona.

c. Procedimientos de reclamación en vía administrativa

Si el ciudadano considera que sus datos no son tratados correctamente y cree que debe ser tutelado en sus derechos, puede acudir al órgano de control de cumplimiento de la Ley (la Agencia Española de Protección de Datos), a solicitar que se atiendan sus reclamaciones encaminadas a hacer efectivo y real el cumplimiento de la norma por el titular del fichero.

De entre estos procedimientos que la Ley contempla en vía administrativa señalamos por su interés el procedimiento de tutela de derechos y el procedimiento sancionador.

[118] *Último párrafo, del apartado tercero, de la norma primera de la Instrucción 1/1998.*

c.1. Procedimiento de tutela de derechos

El ejercicio de los derechos que otorga a los ciudadanos la Ley se lleva a cabo mediante un procedimiento de tutela, que podemos orientar en la línea de lo que se ha dado en llamar el "habeas data", como instrumento que permite facilitar un camino mediante el que el afectado puede ejercer la defensa de los derechos que se pretende proteger[119].

En el caso español, el Real Decreto 1332/1994, de 20 de junio, citado, regula determinados aspectos, *en su mayoría de orden procedimental, referentes al ejercicio de los derechos de acceso, rectificación y cancelación, a la forma de reclamar ante la Agencia Española de Protección de Datos por actuaciones contrarias a la Ley, a la notificación e inscripción de los ficheros automatizados de datos y al procedimiento para la determinación de las infracciones y la imposición de las sanciones.*

El procedimiento de tutela de derechos se encuentra regulado en el artículo 17 del Reglamento, indicando que se debe iniciar siempre a instancia del afectado, mediante escrito de reclamación ante la Agencia Española de Protección de Datos; en el referido escrito se debe indicar con claridad el contenido de su reclamación y los preceptos de la Ley que se consideren vulnerados[120].

Recibida la reclamación se da traslado de la misma al responsable del fichero para que formule las alegaciones que considere convenientes y, tras audiencia al afectado y de nuevo al responsable del fichero, el Director de la Agencia Española de Protección de Datos resolverá dando traslado a los interesados de la resolución, cabiendo recurso contencioso-administrativo contra la misma.

c.2. Procedimiento sancionador

El procedimiento sancionador se encuentra regulado en los artículos 18 y 19 del Reglamento; se inicia siempre de oficio por la Agencia Española de Protección de Datos, bien haya tenido conocimiento por denuncia del afectado o de un tercero, o por otros motivos o actos, como puede ser el ejercicio de la actividad inspectora.

Algo más complejo en su desarrollo que el procedimiento de tutela de derechos, el sancionador se inicia mediante acuerdo del Director de la Agencia Española de Protección de Datos, en el que se designará instructor con indicación de la posibilidad de recusación y se identificará al presunto responsable, o responsables, concretando los hechos y la infracción que, supuestamente, ha cometido, así como la sanción o sanciones que se pueden imponer y las medidas cautelares a adoptar en su caso.

Una vez se notifique al presunto responsable la incoación del expediente, ofreciéndole la posibilidad de efectuar alegaciones y de emplear los medios de prueba de que se quiera valer, se ordenará por el instructor la práctica de las mismas y volverá a poner de manifiesto el expediente al presunto responsable para que, a la vista del resultado de las pruebas, pueda alegar nuevamente, incluso aportando documentos, lo que considere de interés.

Por último, el instructor formulará una propuesta de resolución motivada que notificará al presunto responsable para que, en un nuevo plazo de quince días, pueda formular nuevas alegaciones si lo considera oportuno.

Termina el procedimiento con la notificación al responsable de la resolución que determinará con precisión los hechos imputados, la infracción cometida, el responsable de la misma y la sanción impuesta, o la declaración de no existencia de responsabilidad, expresando también el derecho de interponer contra la misma el correspondiente recurso contencioso-administrativo.

---

[119] *Ya hemos indicado en algún otro comentario a la Ley española –exactamente al proyecto de ley español, pues tal era en aquel entonces– que el procedimiento debe ser tal que su ejercicio no levante sospechas y el cauce procedimental esté suficientemente garantizado, ya que el órgano que se cree para ello, en su caso, si no goza de esa independencia, puede llegar a ser un nuevo santuario burocrático, donde se reciba la esperanza de protección para devolver desengaños traumáticos. Seguimos opinando de la misma forma sobre este tema y lo seguiremos exponiendo. Cfr. Davara, M.A. "Intimidad, informática y seguridad jurídica en España". Boletín de la Fundación para el Desarrollo Social de las Comunicaciones (128) FUNDESCO. Madrid. abril 1992. pg. 14.*

[120] *Nosotros entendemos que lo que debe figurar con claridad es el contenido de su reclamación porque no creemos que se debe dejar de atender una petición de tutela de derechos de un ciudadano porque no vengan expresados "con claridad" los preceptos de la Ley que se consideren vulnerados.*

La calificación de los hechos y, consecuentemente, la sanción a imponer, está resultando tema controvertido pues la Agencia Española de Protección de Datos realiza una interpretación *"sui generis"* de la Ley que ha concluido con la imposición de múltiples multas de elevadas cantidades. La lentitud de los órganos jurisdiccionales, en particular, la Audiencia Nacional, está resultando gravemente dañosa y haciendo, en la práctica, que el órgano de control del cumplimiento de la Ley se haya convertido en un órgano atemorizante, más que en un órgano de apoyo interpretativo y de tutela de derechos.

9. CÓDIGOS TIPO

La LOPD prevé que tanto los responsables de ficheros de titularidad pública como privada puedan elaborar códigos tipo, éticos, deontológicos o de conducta, con el fin de adaptar las disposiciones y la interpretación de la Ley a un sector particular. Esta previsión de la LOPD trae causa de lo dispuesto en el artículo 27 de la Directiva 95/46/CE, en el que se insta a los Estados miembros y a la Comisión Europea a alentar la elaboración de códigos de conducta que permitan una mejor aplicación de las disposiciones nacionales sobre protección de datos teniendo en consideración las particularidades de cada sector.

Estos códigos tipo deben ser inscritos en el Registro General de Protección de Datos, para lo cual es necesario que cumplan con unos requisitos de forma y de fondo, de manera que es necesario que el código aporte un valor añadido al mero cumplimiento de las disposiciones de la LOPD.

10. INFRACCIONES Y SANCIONES

El Título VII de la LOPD, bajo el epígrafe de "infracciones y sanciones", regula (arts. 43 a 49), un régimen sancionador al que estarán sometidos los responsables de los ficheros y en el que se califican las infracciones como leves, graves y muy graves (art. 44), estableciéndose multas que van desde los seiscientos un euros con un céntimo (cien mil pesetas), a los seiscientos un mil doce euros con diez céntimos (cien millones de pesetas), graduándose la cuantía atendiendo a (art. 45.4):

> *"La naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora".*

Las infracciones prescribirán a los tres años las muy graves, a los dos las graves y al año las leves, comenzándose a contar el plazo de la prescripción desde el día en que la infracción se haya cometido y, con relación a las sanciones, también se establece un plazo de prescripción siendo de tres años las que hayan sido impuestas como consecuencia de faltas muy graves, de dos años las consecuentes de faltas graves y de un año las que provengan de faltas leves.

Cuando se cometa una infracción calificada como muy grave, de forma que se estén utilizando o cediendo los datos personales atentando gravemente contra los derechos *"de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan",* el Director de la Agencia Española de Protección de Datos, además de ejercer la potestad sancionadora, podrá requerir a los responsables de los ficheros la cesación de esa ilícita utilización o cesión de datos (art. 49), pudiendo, en caso de no ser atendido en su requerimiento, inmovilizar los ficheros.

Precisamente son las sanciones tan elevadas las que a veces nos llevan a pensar si de verdad esta norma es una norma equilibrada y acorde con el derecho que pretende proteger.

Es cierto que se trata de un derecho fundamental pero también es cierto que somos el país del mundo con sanciones económicas más altas; y, además, con mucha diferencia.

Preguntamos, ¿es lógico que un error informático en el que no exista mala fe pueda llevar, por cada caso denunciado, a una sanción de hasta seiscientos mil y pico euros, esto es, de hasta cien millones de pesetas?

No queremos dar respuesta a la pregunta ya que no es éste el objeto de la obra, pero sí queremos llamar la atención a los responsables de las empresas sobre que las multas se están aplicando con rigor y no hay más que leer las anuales memorias de la Agencia Española de Protección de Datos para comprobar que esto es así.

Cuando menos se lo piensa uno se encuentra con una sanción, de elevada cuantía, que hace que nos planteemos muchas preguntas; pero no es el lugar, ni el momento, para seguir con esta argumentación.

Cumplamos con la protección de datos porque es un derecho fundamental de todos y debemos respetar los principios y el ejercicio de los derechos de los interesados que hemos expuesto. Cumplamos con la protección de datos porque es nuestra obligación cumplir con todas las normas y porque ésta, además, se presenta como una garantía de seguridad y de desarrollo de nuestra empresa sin problemas añadidos.

De esta forma, cumpliendo con la protección de datos, además evitaremos fuertes sanciones.

11. TRANSFERENCIA INTERNACIONAL DE DATOS

El desarrollo global del comercio, y más en concreto la plasmación que ha tenido en un fenómeno social como es el comercio electrónico, y la presencia de las multinacionales tanto en Estados Unidos, principalmente, como en la Unión Europea, ha supuesto la necesidad de arbitrar una serie de normas que regulen la transmisión de datos personales entre entidades que pueden encontrarse en cualquier parte del mundo.

Muestra de lo anterior ha sido la publicación de varias Decisiones por parte de la Comisión de las Comunidades Europeas con terceros países para garantizar la protección de los datos y, en concreto, la Decisión sobre el Acuerdo de Puerto Seguro que regula las transferencias internacionales de datos que tengan por destino a entidades norteamericanas que se hayan adherido a dicho sistema.

Además de la anterior, la Comisión Europea ha aprobado Decisiones relativas al nivel de protección de datos adecuado conferido por Hungría[121], Suiza, Canadá, Argentina, Bailía de Guernsey e Isla de Man, lo que supone que puedan llevarse a cabo transferencias de datos desde un Estado miembro de la Unión Europea con destino a alguno de estos países sin mayores dificultades.

Asimismo, la Comisión Europea ha elaborado dos Decisiones relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países, en virtud de las cuales podrán transferirse datos, de un lado, entre un responsable del tratamiento situado en la Unión Europea y un destinatario de los mismos que se encuentre en un tercer Estado y, de otro lado, entre un responsable del fichero establecido en un Estado miembro de la Unión Europea y un encargado del tratamiento establecido en un tercer país, garantizando al titular de los datos una protección mínima y necesaria conforme a lo dispuesto en la normativa comunitaria. Y ello, sin perjuicio de la posibilidad de realizar dichas transferencias mediante otros contratos, siempre y cuando se haya obtenido la autorización previa de la Agencia Española de Protección de Datos.

[121] Actualmente, la Decisión por la que se declaraba a Hungría como un país con nivel adecuado de protección ha perdido su fundamento puesto que recientemente Hungría ha entrado a formar parte de la Unión Europea.

En particular, a la transferencia de datos entre distintos países dedica la LOPD el Título V que, bajo el epígrafe de "Movimiento internacional de datos", contiene los artículos 33 y 34 bajo la teoría general de que no podrán realizarse transferencias temporales ni definitivas con destino a otros países que no proporcionen un nivel de protección equiparable al que presta nuestra Ley y siempre se realizarán con la autorización previa del Director de la Agencia Española de Protección de Datos que deberá asegurarse de que existen las garantías suficientes.

A esta norma general, se establecen algunas excepciones con base en 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, cuando se refiera a transferencias dinerarias conforme a su legislación específica, o cuando el interesado haya dado su consentimiento, cuando 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 propio interesado.

Para conocer cómo se deben interpretar estas normas, de acuerdo con la línea doctrinal seguida por la Agencia Española de Protección de Datos, y tener la garantía de que cuando transferimos datos a terceros países lo estamos haciendo sin riesgo de incumplimiento de la norma y, por tanto, sin riesgo a ser sancionados, se debe acudir a la Instrucción 1/2000[122] relativa a la transferencia internacional de datos centrada en las características que, en opinión del Director de la Agencia Española de Protección de Datos, se deben contemplar en el momento en que necesitemos realizar una transferencia de datos a otro país.

La referida Instrucción en su norma segunda indica que

> *La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento.*

Con el estudio y aplicación del resto de la Instrucción, comprobamos que si se cumple con la garantía de los principios de la protección de datos y los derechos de las personas, contemplados en la LOPD, es posible que no se burle la protección en la transferencia internacional realizada a un Estado que forme parte de la Unión Europea, o a un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado, pero también sirve el análisis de la Instrucción para conocer cuáles son las posibilidades que ofrece la Ley para transferir datos a otros países en los que no exista ninguna protección.

12. PROTECCIÓN DE DATOS E INTERNET

Vista la importancia que adquiere la protección de datos, como garantía de una correcta actuación por parte de quien trata los datos y del respeto que puede esperar el titular de los mismos, se hace imprescindible recordar que en el tratamiento de datos efectuado a través de Internet u otros medios de comunicación electrónica también tiene que garantizarse la aplicación tanto de la normativa comunitaria en la materia, como de las normas que regulan en nuestro Ordenamiento jurídico la protección de datos igual al que tienen en otros ámbitos.

Es necesario tomar en consideración que en Internet aparecen sujetos específicos, tales como la operadora de telecomunicaciones, el proveedor de acceso a Internet o el proveedor de servicios de Internet, que para el desarrollo de su actividad y la prestación de sus servicios requieren del tratamiento de los datos de los usuarios, y que por tanto, quedan sometidos a la normativa sobre protección de datos general y específica en el sector de las telecomunicaciones (comunicaciones electrónicas).

[122] *Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, publicada en el Boletín Oficial del Estado número 301, de 16 de diciembre.*

Al igual que ocurre en el entorno no electrónico o físico *(off line),* la protección de datos en Internet se convierte en una obligación para quienes tratan datos de los usuarios y en una garantía para estos últimos. Si bien dicha protección habrá de ser el resultado de una combinación entre las disposiciones legales, recordando que no todos los ordenamientos jurídicos tratan la cuestión de la misma forma, y las diferentes soluciones tecnológicas que desde la industria del hardware y software se desarrollen para dar soluciones específicas a esta cuestión. Un claro ejemplo de esto último puede verse, entre otros, en la Plataforma de Preferencias de Privacidad (P3P) que ayudaría a quienes recaban datos a cumplir la normativa, y a los usuarios que los proporcionan a estar mejor informados y poder tomar las decisiones oportunas.

13 RÉGIMEN SANCIONADOR

Sin intención de convertir el régimen sancionador en una de las razones para el cumplimiento de la Ley, ya que debe recordarse una vez más que el tratamiento efectuado por el responsable del fichero debe ser no sólo legal sino también leal lo que supone que no se incurriera en ninguna infracción, sí debe mencionarse que la infracción de alguna de las normas por parte de quien trata datos de carácter personal lleva aparejadas sanciones que van desde los 601,01 euros (100.000 pesetas) hasta los 601.012 euros (cien millones de pesetas), en el caso de ficheros de titularidad privada, y podrá suponer la iniciación de las actuaciones disciplinarias correspondientes cuando se trate de ficheros de los que sea responsable la Administración Pública.

En virtud de lo dispuesto en la ley están sujetos al régimen sancionador tanto el responsable del fichero como el encargado del tratamiento, lo que supone que tengan que responder personalmente por las infracciones en que hubieran incurrido al tratar datos de carácter personal.

Cabe señalar que las infracciones se clasifican en leves, graves y muy graves. Por lo que se refiere a su prescripción, las infracciones muy graves prescriben a los tres años, las graves a los dos años y las leves al año, comenzando a contarse el plazo de prescripción desde el día en que la infracción se hubiera cometido.

Por último, el procedimiento sancionador se encuentra regulado en los artículos 18 y 19 del 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, subsistente en virtud de la Disposición Transitoria tercera de la LOPD.