La protección de datos de carácter personal en Internet (con especial especial referencia a la transferencia internacional de datos)

ALFONSO ORTEGA GIMÉNEZ

SUMARIO

CAPÍTULO SEGUNDO

INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS Y RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS

CAPÍTULO TERCERO

TRANSFERENCIA INTERNACIONAL DE DATOS

INTRODUCCIÓN.

I. Como consecuencia de las grandes inversiones tecnológicas realizadas en infraestructuras de información y comunicación, desde hace un par de décadas, se fue allanando el camino hacia la construcción de lo que hoy denominamos "Sociedad de la Información", que ha permitido la creación de nuevas esferas de intercambio cultural y social, provocando cambios, no sólo en la manera en que se relacionan las personas sino también en la forma de hacer negocios o de gestionar una empresa.

Es evidente que la "Sociedad de la Información", en el afán de gestionar la transmisión de la información y considerando, que hoy en día, el conocimiento se ha convertido en un importante recurso productivo, ha encontrado en *Internet* un canal de comunicación rápido, barato y eficiente. *Internet* es el motor de la transformación de la práctica empresarial ya que ha pasado de ser una estrategia de difusión o un canal de ventas a convertirse en un medio que permite prácticamente todo tipo de relación comercial. El hecho de que *Internet* permite a ordenadores de todo tipo comunicarse y compartir servicios de manera directa y transparente a lo largo y ancho del mundo lo ha convertido en un enorme valor, en un importante recurso de información y en un instrumento de cooperación y colaboración internacional.

Internet no es algo pasajero sino que es un fenómeno tan amplio que no vale simplemente conectarse para hacerse una idea de sus dimensiones y su repercusión, sino que, una vez conectado, hay que internarse muy bien para captar su esencia. Ahora bien, no es menos cierto que la implantación de *Internet* está provocando un profundo debate acerca de cuestiones tales como cuál es el tratamiento que se debe dar a la información confidencial, cómo podemos evitar el fraude en las transacciones comerciales o qué soluciones podemos dar a la piratería informática; en definitiva, se hace necesario un esfuerzo no sólo por parte de los Estados sino por parte de todos los que, de una manera u otra, nos vemos afectados por este fenómeno, con el fin de dotar a *Internet* de un marco jurídico que otorgue a los usuarios, algo tan sencillo de pedir pero a la vez tan complejo de conseguir como es la seguridad jurídica.

II. Los objetivos de esta obra son dos: primero, abordar la problemática que presenta la relación entre *Internet* y la protección de datos de carácter personal; y, segundo, en este contexto tan "internacional" hacer un breve análisis acerca de la transferencia internacional de datos.

Es necesario reflexionar acerca de la protección de datos de carácter personal en el ámbito de *Internet*. El derecho a la intimidad de las comunicaciones electrónicas es un derecho fundamental que, hoy en día, se está viendo amenazado ya que cada vez que nosotros utilizamos el *email*, participamos en un Grupo de noticias o simplemente estamos navegando por *Internet*, estamos revelando, de forma involuntaria y sin darnos cuenta, toda una serie de datos, acerca de nuestro sistema operativo, de nuestro navegador y de las *webs* que hemos visitado, e incluso datos de nuestra personalidad, nuestros gustos o de nuestra situación económica.

El segundo objetivo no puede ser otro que el análisis del régimen de la transferencia internacional de datos, pues, a pesar de que el criterio general en esta materia es la prohibición de las transferencias al extranjero de datos de carácter personal que hayan sido objeto de tratamiento cuando el país de destino no tenga un nivel de protección equiparable al de la LOPD, veremos que, como consecuencia de la normativa convencional e institucional existente en la materia, a diario se suceden, por ejemplo, la remisión de datos de carácter personal de los trabajadores a países, no sólo comunitarios, sino extracomunitarios, tales como EE.UU., Canadá o Suiza con la finalidad de ser allí objeto de tratamiento.

III. Esta obra se divide en dos partes fundamentales. En primer lugar, trataremos de abordar la problemática que presenta la relación entre *Internet* y el derecho a la protección de datos de carácter personal. Se trata, una vez más, de dar solución a los principales problemas que se plantean en este ámbito, reflexionando acerca de qué podemos entender por derecho fundamental a la protección de datos de carácter personal, en qué consiste el tratamiento de datos de carácter personal, cuáles son los niveles de seguridad aplicables a los ficheros de tratamiento de datos de carácter personal, o cuál es el régimen jurídico del tratamiento de datos de carácter personal efectuado a través de *Internet*. Y, finalmente, en la segunda parte, vamos a analizar el régimen de la transferencia internacional de datos, a través de las respuestas que vamos a tratar de dar a las dos cuestiones siguientes: por un lado, cuál es el régimen de la transferencia internacional de datos que se prevé en la LOPD; y, por otro lado, teniendo en cuenta que desde la UE el principal destino de los datos de carácter personal son los EE.UU., analizaremos cómo se debe realizar la transferencia de datos de carácter personal a entidades ubicadas en los EE.UU.

Alicante, 29 de julio de 2003

CAPÍTULO PRIMERO
LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO DE INTERNET

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL[1].

1. La protección de la intimidad y el secreto de las comunicaciones son derechos constitucionalmente reconocidos, cuya relevancia nadie pone en duda. Se encuentran entre los considerados derechos fundamentales, en relación con los que el artículo 10.1 de la CE señala que "la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social" y, en el artículo 18.4 de la CE se establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Pues bien, la protección de la intimidad y de los derechos a ella ligados plantea retos cada vez más novedosos, en la medida en que las nuevas tecnologías de la información permiten no sólo nuevas formas de comunicación, sino también, paralelamente, más modos de interceptar las comunicaciones. Ahora bien, como ya hemos visto, el Derecho ha reaccionado ante los retos planteados por las nuevas tecnologías.

La información se ha convertido en uno de los valores más codiciados y valorados en Internet. Los datos constituyen la materia prima de muchos negocios, como es el caso de las empresas de marketing directo y publicidad, sin embargo también lo son de muchas actividades ilícitas, como es el caso de la venta de números de tarjetas de crédito[2].

---

[1] Vid. ÁLVAREZ CIVANTOS, Oscar José, Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades, Editorial Comares, Granada, 2001, pp. 5-42.

[2] El mercado criminal de venta de números de tarjetas de crédito alcanza día a día proporciones crecientes. Cada semana, datos robados de decenas de miles de tarjetas de crédito se ofrecen al mejor postor en ciberbazares operados en su mayoría por residentes de la antigua Unión Soviética. El sector financiero calcula que las pérdidas ocasionadas por los ciberdelincuentes superan anualmente los 1.000 millones de dólares. En este mercado negro y siniestro se comercia igualmente con todo tipo de datos personales. Según señalaba la semana pasada The New York Times, el precio de los datos fluctúa a diario, según la oferta, que parece ser interminable y creciente. El precio puede ir desde los 40 centavos de dólar hasta los 5 dólares, dependiendo del nivel de autentificación logrado. Normalmente, los datos se ofrecen en paquetes, por ejemplo, 250 tarjetas a 100 dólares, o 5.000 tarjetas a 1.000 dólares, y se cobran a través de cuentas online en servicios como www.WebMoney.ru que hace posible la transferencia a depósitos bancarios. El consumidor final está protegido ya que debe validar los cargos bancarios, esto es, está protegido del fraude siempre que rechace a tiempo el cargo que viene en el extracto bancario. Sin embargo, expertos consultados señalan que la criminalidad hace aumentar los tipos de interés, lo que termina por perjudicar al usuario. Los compradores que acuden a foros y chats de *Internet* proceden de todo el mundo, aunque destaca la presencia de demandantes de la exUnión Soviética (sobre todo, Rusia y Ucrania), Europa del Este, Asia y, especialmente, Malasia. El destino de los datos va desde compras en tiendas *online* de Occidente hasta la extracción de dinero en cajeros automáticos.

2. Es hora de reflexionar en profundidad en el objeto principal de este estudio: el análisis de la protección de datos de carácter personal en el ámbito de *Internet*. A continuación, vamos a tratar de abordar la problemática que presenta la relación entre *Internet* y el derecho a la protección de datos de carácter personal. Se trata, una vez más, de dar solución a los principales problemas que se plantean en este ámbito, reflexionando acerca de qué podemos entender por derecho fundamental a la protección de datos de carácter personal, en qué consiste el tratamiento de datos de carácter personal, cuáles son los niveles de seguridad aplicables a los ficheros de tratamiento de datos de carácter personal, o cuál es el régimen jurídico del tratamiento de datos de carácter personal efectuado a través de *Internet*.

1. Normativa aplicable en materia de protección de datos de carácter personal.

3. El marco habilitante del desarrollo de la normativa sobre protección de datos de carácter personal nos lo proporciona la CE que, en su artículo 18.4, establece que "*la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". La columna vertebral de la regulación del derecho fundamental a la protección de datos de carácter personal está integrada por las siguientes normas:

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[3].

- Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[4].

- Convenio 108/81/CE del Consejo, de 28 de enero, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

[3] *DOCE* núm. L 201, de 31 de julio de 2002.
[4] *DOCE* núm. 24, de 30 de enero de 1998.

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

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal[5].

4. Ahora bien, junto a estas normas podemos citar, además de las diferentes Instrucciones dictadas por la APD desde el año 1995 y de los diferentes Documentos del Grupo del artículo 25 de la Directiva 95/46/CE, las siguientes normas que permanecen vigentes:

- Carta de los Derechos Fundamentales de la Unión Europea.

- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos[6].

- 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[7].

- Orden de 2 de febrero de 1995, por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos[8].

- Orden de 31 de julio de 1998, por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos[9].

2. Concepto del derecho fundamental a la protección de datos de carácter personal.

5. El derecho fundamental a la protección de datos de carácter personal es un derecho fundamental independiente del derecho al honor y a la intimidad familiar y personal, al domicilio y a las comunicaciones; se trata de un derecho con caracteres propios, que no se presenta ya como instrumental del resto de derechos, sino como un derecho independiente,

[5] *BOE* núm. 151, de 25 de junio de 1999.
[6] *BOE* núm. 106, de 4 de mayo de 1993.
[7] *BOE* núm. 147, de 21 de junio de 1994.
[8] *BOE* núm. 35, de 10 de febrero de 1995.
[9] *BOE* núm. 200, de 21 de agosto de 1998.

cuyo límite se encuentra, precisamente, en el juego del resto de derechos fundamentales y bienes jurídicos constitucionalmente protegidos[10].

El derecho a la protección de datos, que engloba el derecho a conocer quién almacena nuestros datos y con qué finalidad, y los derechos a acceder, rectificar, oponernos y cancelar aquellos de nuestros datos que hemos permitido sean tratados, es el derecho de toda persona al control y disposición sobre sus datos personales, que deberá protegerse por los poderes públicos y asimismo, impone a terceros la realización de cuantos comportamientos sean necesarios para no invalidarlos.

Este derecho a la protección de datos, al que algunos autores prefieren denominar "derecho fundamental de la libertad informática", ha sido considerado como derecho fundamental superior al contenido del mencionado artículo 18.4 de la CE.

3. Sujetos obligados a cumplir la normativa sobre protección de datos de carácter personal.

6. La LOPD define, en su artículo 3.d), como sujeto al que son directamente aplicables sus disposiciones la figura del *"responsable del fichero o tratamiento"*, a aquella *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*.

Como contraposición de esta figura aparece la del *"afectado o interesado"*, que será, según el artículo 3.e) de la LOPD, aquella *"persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo"*.

4. Concepto de datos de carácter personal.

7. De acuerdo con el artículo 3.a) de la LOPD, por dato de carácter personal debemos entender *"cualquier información concerniente a personas físicas identificadas o identificables"*. Más explícito es el artículo 1 del Real Decreto 1332/1994, de 20 de junio, al disponer que son datos de carácter personal *"toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"*. Este amplio concepto, permite incluir como datos de carácter personal el D.N.I. o N.I.F., los números de la

[10] En el mismo sentido, la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000.

Seguridad Social o de la mutualidad, el nombre y apellidos, la dirección, el teléfono, el lugar y la fecha de nacimiento, el sexo o la nacionalidad. Ahora bien, no se incluyen en este concepto los datos referidos a personas jurídicas, ya que lo que se protege con esta normativa es la intimidad y el honor de las personas físicas.

5. Principios rectores en materia de protección de datos de carácter personal.

8. La LOPD establece en su Título II bajo la expresión "Principios de la protección de datos" los siguientes apartados: a) Calidad de los datos (artículo 4 de la LOPD); b) Consentimiento del afectado (artículo 6 de la LOPD); c) Datos especialmente protegidos (artículo 7 de la LOPD); d) Datos relativos a la salud (artículo 8 de la LOPD); e) Seguridad de los datos (artículo 9 de la LOPD); f) Deber de secreto (artículo 10 de la LOPD); g) Comunicación de datos (artículo 11 de la LOPD); h) Acceso a los datos por cuenta de terceros (artículo 12 de la LOPD). Ahora bien, podríamos resumir estos derechos y obligaciones en los siguientes:

A) Principio de finalidad y adecuación del tratamiento:

Este principio implica que cualquier sujeto, ya sea persona física o jurídica, que ocupe la posición de responsable del fichero y asuma la recogida, almacenamiento, archivo o agrupación de datos de personas físicas, deberá hacerlo en aras a una finalidad concreta, explícita y legítima, que será la que determine el tratamiento.

Los ficheros nacen con una finalidad concreta, que será la que se comunique al afectado y sobre la que recaerá el consentimiento de aquel para el tratamiento.

B) Principio de libre disposición y control sobre sus datos por el afectado:

El eje central del principio de libre disposición y control de sus datos por el afectado lo encontramos en dos derechos consecutivos y complementarios: el derecho de información del interesado, que se convierte en deber ineludible del responsable del fichero; y, el del consentimiento del interesado, que constituye la autorización para realizar el tratamiento, con el contenido del que el interesado ha sido informado.

Así, la primera manifestación de este principio la encontramos en el artículo 5 de la LOPD que exige que a los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco, entre otros, de la existencia del fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos, de

los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean formuladas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y, de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

La segunda manifestación del principio de libre disposición y control sobre sus datos por el afectado aparece en el artículo 6 de la LOPD al establecer que *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*.

C) Principio de veracidad y exactitud de los datos:

El responsable del fichero tiene la obligación de mantener los datos exactos y verdaderos en la medida en que es el propio artículo 4.3 de la LOPD el que señala que *"los datos de carácter personal serán exactos y puestos al día de forman que respondan con veracidad a la situación actual del afectado"*.

D) Principio de licitud y legalidad del tratamiento:

Cualquier tratamiento de datos debe cumplir con las exigencias contenidas en la normativa sobre protección de datos de carácter personal, esto es, con lo previsto tanto en la LOPD como en su legislación complementaria; de ahí que sea el propio principio de licitud y legalidad del tratamiento el que nace con la finalidad de garantizar la efectividad del derecho a la protección de datos de carácter personal.

En definitiva, podemos llegar a la conclusión de que el principio de legalidad y licitud del tratamiento es un complemento de los principios anteriores ya que el efectuar el tratamiento sin respetar la finalidad del mismo y el no permitir al interesado ejercer el control y disposición sobre sus datos, convierte el tratamiento en ilícito, con la consiguiente sanción para el responsable del fichero.

E) Principio de seguridad y confidencialidad del tratamiento:

Los principios de seguridad y confidencialidad del tratamiento imponen al responsable del fichero un deber de diligencia dirigido a evitar que los datos escapen de su esfera pudiendo llegar a manos de personas no autorizadas, o a perderse o destruirse.

A estos principios se refiere tanto la LOPD en sus artículos 9 y 10 como el RMS con el objeto de que en los tratamientos automatizados se adopten las medidas necesarias para salvaguardar la seguridad de los datos.

F) Principio de control administrativo**:**

El cumplimiento de los principios anteriormente expuestos, según se deduce del artículo 37 de la LOPD, queda en manos de la Agencia de Protección de Datos, ente de derecho público, con personalidad jurídica propia y plena capacidad tanto pública como privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones, ya que a este órgano le corresponde velar por la aplicación de la normativa y por el respeto a los derechos de los afectados por el tratamiento.

La APD, que en su estructura integra al RGPD, es el órgano encargado de inspeccionar y controlar el cumplimiento de la LOPD y de la legislación complementaria, y velar por los intereses de los ciudadanos, que pueden dirigir a este órgano las reclamaciones que tengan sobre el tratamiento de sus datos.

II. EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL[11].

1. Creación de ficheros de tratamiento de datos de carácter personal.

9. La recogida de datos de carácter personal por cualquier entidad se ha convertido en algo habitual de un tiempo a esta parte, a la hora de prestar un servicio público, cuando se realiza un trabajo de investigación o al hilo de la firma de un contrato. Estos datos que se recogen con una finalidad preestablecida, se incorporan a ficheros que son fácilmente transmisibles a través de las nuevas tecnologías de la información, quedando la titularidad de los mismos en manos de las entidades que los han recopilado.

Los ficheros de datos creados pueden ser, entonces, de titularidad pública o de titularidad privada pero, una cosa si debe quedar clara: la obtención, uso, conservación y almacenamiento de los datos debe estar presidida por el "Principio de calidad de los datos", que supone la necesidad que tienen los responsables de los datos y los encargados de su tratamiento de especificar la finalidad para la que se solicitan, obtenerlos de manera lícita, actualizar el fichero,

[11] *Vid.* ÁLVAREZ CIVANTOS, Oscar José, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Editorial Comares, Granada, 2001, pp. 43-111.

utilizar los datos de acuerdo con la finalidad para la que se obtuvieron, cancelarlos cuando sea pertinente y registrarlos de forma que permitan el ejercicio del derecho de acceso, rectificación y cancelación.

2. El derecho de información en la recogida de datos.

10. Según el artículo 5 de la LOPD, toda persona física o jurídica que solicite datos de carácter personal a otras personas para su almacenamiento y tratamiento en un fichero, automatizado o no, deberá informarlas de modo expreso, preciso e inequívoco de los siguientes aspectos:

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

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

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

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición al almacenamiento o tratamiento de sus datos.

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

Existen diferentes formas de cumplir con ese deber de información que establece el artículo 5 de la LOPD, a saber:

a) En el propio formulario de recogida de datos dispuesto al efecto.

b) En un lugar visible en el lugar en el que se realice la recogida de datos, tanto si es físico como virtual.

c) De palabra.

d) Por medio de una notificación con acuse de recibo.

3. El consentimiento del afectado por el tratamiento de sus datos.

11. En materia de protección de datos de carácter personal, es esencial el consentimiento del afectado por el tratamiento. Toda entidad que pretenda tratar datos de personas físicas deberá requerirles previamente su consentimiento para el tratamiento, salvo que los datos se hayan recogido como consecuencia de una relación contractual o precontractual, o que se encuentren en algunos de los supuestos legales que eximen del mismo.

La LOPD define, en su artículo 3.h), el consentimiento del interesado como "*toda manifestación de voluntad, libre, inequívoca, específica e informad, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"*. Así, contenido mínimo del consentimiento son las distintas formas que se exigen en función de los datos objeto del tratamiento, a los que, además, debemos añadir la dificultad que plantean las nuevas formas de consentimiento surgidas al amparo de las nuevas tecnologías de la información y, particularmente, en lo que se refiere a manifestaciones de voluntad efectuadas por medios electrónicos.

En función del tipo de datos que vayan a ser objeto del tratamiento, la LOPD determina la necesidad de una u otra forma de consentimiento, del siguiente modo:

a) Datos de carácter personal que revelen la ideología, afiliación sindical, religión o creencias: para estos datos se exigirá el consentimiento expreso y por escrito, salvo cuando los responsables del fichero sean partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad de tratamiento sea política, filosófica, religiosa o sindical., en cuanto a los datos relativos a sus asociados o miembros, que únicamente necesitarán el consentimiento para el caso de cesión de los datos recogidos.

b) Datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual: para estos datos se requerirá el consentimiento expreso del afectado o la autorización concedida por una norma con rango de Ley por razones de interés general.

c) Datos de carácter personal no incluidos en los grupos anteriores: para la recogida de los datos de carácter personal no incluidos en los dos grupos anteriores, el tipo de consentimiento requerido será e mismo al que hace referencia el artículo 3.h) de la LOPD, esto es, un

consentimiento libre, inequívoco, específico e informado, mediante el cual el interesado manifieste su conformidad con el tratamiento de datos de carácter personal que le conciernen.

Parece evidente que si en los datos recogidos en los dos primeros grupos el único consentimiento admitido será el expreso y que para los datos referidos a la ideología, afiliación sindical, religión o creencias, éste deberá ser escrito, para el resto de datos la LOPD no establece la obligación de que el consentimiento sea expreso, sino únicamente que este sea inequívoco y específico; por tanto, la LOPD admite tanto el consentimiento expreso como el consentimiento tácito.

12. Al igual que hicimos en su momento con el deber de información, es recomendable analizar las distintas formas de consentimiento para conocer cual de ellas se adapta a cada uno de los niveles de seguridad fijados por la normativa sobre protección de datos de carácter personal:

a) Consentimiento escrito y expreso: es necesario para el tratamiento de datos de carácter personal relativos a la ideología, afiliación sindical, religión o creencias.

b) Consentimiento de palabra o verbal: este tipo de consentimiento sería válido para el tratamiento de datos relativos a la salud, al origen racial y a la vida sexual, pero no para los datos concernientes a la ideología, afiliación sindical, religión y creencias.

c) Consentimiento electrónico: este tipo de consentimiento se puede manifestar de las siguientes formas: primero, mediante la firma electrónica; segundo, por medio del correo electrónico; y, tercero, por medio de campos o pestañas dispuestas al efecto.

d) El silencio como forma de consentimiento: el silencio se puede considerar como consentimiento inequívoco, cuando existe una obligación de contestar por parte del afectado.[12] Ahora bien, el silencio como forma de prestar el consentimiento, no podrá alcanzar, el carácter de consentimiento expreso, sino simplemente el de consentimiento tácito e inequívoco, por lo que será válido en lo que respecta a los datos que requieren los niveles de seguridad básico y medio, pero nunca los de nivel alto, es decir, no será válido para consentir el tratamiento o cesión de datos de afiliación sindical, religión o creencias, origen racial, salud y vida sexual.

[12] Así lo ha puesto de manifiesto el propio Tribunal Supremo en las SSTS de 18 de marzo de 1994, y de 22 de noviembre de 1994.

13. Lo anteriormente expuesto lo debemos relacionar con el artículo 6 de la LOPD, que establece una serie de excepciones al consentimiento del afectado, que se pueden concretar en las siguientes:

1º) Que una Ley disponga que no es necesario el consentimiento inequívoco del afectado para el tratamiento de sus datos en el ámbito o materia determinados.

2º) Cuando los datos sean recogidos por las Administraciones públicas en el ejercicio de sus competencias y funciones propias.

3º) Cuando se refieran a las partes de un contrato o precontrato en una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

4º) Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado, por la prevención o diagnóstico médicos.

5º) Cuando 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 tercero a quién se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Finalmente, el citado artículo 6 de la LOPD, en su párrafo 4, concede al afectado por el tratamiento la posibilidad de que, en los casos en que no sea necesario su consentimiento, y siempre que una Ley no disponga lo contrario, pueda oponerse al tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal, estando obligado el responsable del fichero, en tal caso, a excluir el tratamiento de los datos relativos al afectado. Además, en su párrafo 3, el artículo 6 de la LOPD establece el carácter revocable del consentimiento.

4. Derechos del afectado por el tratamiento de sus datos.

14. Los afectados o interesados por el tratamiento de sus datos, ostentan los derechos de acceso, rectificación, cancelación y oposición, que presentan los siguientes caracteres comunes:

a) Los derechos indicados son personalísimos, por lo que, en principio, solamente podrían ser ejercitados por el afectado frente al responsable del fichero.

b) Los derechos se configuran como independientes, de forma que no será necesario el ejercicio del derecho de acceso como previo al de los derechos de rectificación y cancelación.

c) Su ejercicio será gratuito, sin que quepa exigir contraprestación alguna por parte del responsable del fichero.

Veamos cada uno de estos derechos:

1º) Derecho de acceso:

Según se desprende del artículo 15 de la LOPD, es facultad del interesado la de solicitar y obtener de forma gratuita del responsable del fichero información acerca de:

1) Sus datos de carácter personal sometidos a tratamiento.
2) El origen de dichos datos.
3) Las comunicaciones realizadas o que se prevean realizar de esos datos.

El ejercicio del derecho de acceso se llevará a cabo mediante una solicitud dirigida al responsable del fichero que contendrá:

1) Datos de identificación del afectado (nombre, apellidos, fotocopia del D.N.I.) y su domicilio a efectos de notificaciones.
2) Petición de acceso con indicación del fichero o ficheros a consultar.
3) Fecha y firma del solicitante.

Según establece el artículo 15.3 de la LOPD, este derecho sólo podrá ser ejercitado en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo, en cuyo caso podrá ejercitarlo antes.

Al ejercitar su derecho de acceso, el afectado podrá elegir alguno de los sistemas de consulta siguientes, siempre que la configuración del fichero lo permita:

1) Visualización en pantalla.
2) Escrito, copia o fotocopia remitida por correo.
3) Telecopia.

4) Cualquier otro procedimiento adecuado a la configuración del fichero, ofrecido por su responsable.

En cuanto a la denegación del derecho de acceso cabe distinguir entre ficheros de titularidad pública o privada:

1) Ficheros de titularidad privada:

En estos casos, la denegación se producirá:

a) Cuando la solicitud sea formulada por persona distinta del afectado.
b) Cuando la solicitud se haya efectuado en un intervalo inferior a doce meses sin acreditar interés legítimo.

2) Ficheros de titularidad pública:

a) En relación con los Ficheros de las Fuerzas y Cuerpos de Seguridad, con fines policiales en función de los peligros que pudieran derivarse para:

- La defensa del Estado.
- La seguridad pública.
- La protección de derechos y libertades de terceros.
- Las necesidades de investigaciones que se estén realizando.

b) En relación con los Ficheros de la Hacienda Pública, cuando el acceso obstaculice:

- Las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias.
- Cuando el interesado esté sometido a actuaciones inspectoras.

c) En general, cuando la información afecte a la defensa del Estado, a la seguridad pública o a la persecución de infracciones penales.

Ahora bien, si la resolución fue estimatoria, el acceso se realizará en el plazo de diez días siguientes a la notificación de aquélla. La información que facilite el responsable del fichero deberá proporcionarse en forma legible e inteligible y comprenderá:

- Todos los datos de base del afectado.
- Los datos resultantes de cualquier elaboración o proceso informático.
- El origen de los datos.
- Los cesionarios de los mismos.
- La especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Si los datos provienen de fuentes diversas, deberán especificarse las mismas señalando la información que proviene de cada una de ellas. Cuando el tratamiento tenga fines de publicidad y prospección, el interesado, al ejercitar su derecho de acceso, tendrá derecho a conocer el origen de sus datos de carácter personal, así como del resto de la información a la que nos hemos referido.

2º) Derecho de rectificación y cancelación:

Tal y como se desprende del artículo 16.2 de la LOPD, el derecho de rectificación y cancelación, puede definirse como la facultad que tiene el interesado de solicitar al responsable del fichero de forma gratuita que por aquél se proceda a corregir o suprimir los datos contenidos en un fichero, en particular, cuando los mismos resulten inexactos o incompletos.

El ejercicio del derecho de rectificación y cancelación se llevará a cabo mediante una solicitud dirigida al responsable del fichero, que contendrá:

1) Datos de identificación del afectado (nombre, apellidos, fotocopia del D.N.I.) y su domicilio a efectos de notificaciones.
2) Petición concreta de rectificación o cancelación.
3) Fecha y firma del solicitante.

La solicitud de rectificación deberá señalar el dato erróneo y la corrección que debe efectuarse, debiendo ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que dependa exclusivamente del consentimiento del interesado. En la solicitud de cancelación, el interesado en la solicitud deberá indicar si revoca el consentimiento otorgado, si procede la revocación, o si la cancelación se funda en que se trata de un dato erróneo o inexacto, en cuyo caso irá acompañado de la documentación justificativa de ese extremo.

El responsable del fichero deberá hacer efectivos los derechos de rectificación y cancelación en el plazo de diez días, utilizando cualquier medio que acredite el envío y la recepción. El plazo se computará desde la recepción de la solicitud o de la subsanación de los defectos. Transcurrido ese plazo, el interesado podrá considerar desestimada su petición, a los efectos de recabar la tutela de la APD.

La LOPD y sus normas de desarrollo establecen una serie de excepciones a los derechos de rectificación y cancelación. Además de las ya señaladas al referirnos al derecho de acceso, en relación con los ficheros de titularidad pública, deben señalarse las siguientes:

a) Cuando la solicitud sea formulada por persona distinta del afectado.
b) Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre el responsable del fichero y el interesado.
c) La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado.
d) No cabrá la rectificación cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, dado que los datos se considerarán exactos si coincidieran con éste.

Si el responsable del fichero considera que no procede atender a la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de diez días siguientes a la recepción de la misma, a fin de que por el interesado pueda recabarse la tutela de la APD.

La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se recojan las bajas producidas. No obstante, el artículo 16.3 de la LOPD prevé que *"la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de la Administraciones Públicas, Jueces y Tribunales, para la atención de las responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas"*. Cumplido el plazo de prescripción se procederá a su supresión. Además, si los datos rectificados o cancelados hubieran sido cedidos o comunicados previamente, el responsable del fichero deberá notificar la rectificación o cancelación realizada al cesionario, a fin de que el mismo, en caso de mantener un tratamiento de los datos, proceda a su rectificación o cancelación.

3º) Derecho de oposición:

Según el artículo 6.4 de la LOPD, *"en los casos en 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 el tratamiento de los datos relativos al afectado"*. Por tanto, son características de este derecho:

1ª) Que se ejercerá en los supuestos en que el tratamiento no requiera el consentimiento del afectado.

2ª) Que la Ley no impida el ejercicio de este derecho.

3ª) Que se alegue un motivo fundado y legítimo, basado en una situación personal del afectado, que justifique la exclusión del tratamiento de sus datos.

5. Cesión de datos a terceros.

15. En virtud del artículo 11 de la LOPD, los datos objeto de almacenamiento o tratamiento sólo podrán ser comunicados o cedidos a terceros, si la cesión tiene por objeto el cumplimiento de fines directamente relacionados con las funciones de la entidad que los cede, y siempre con el previo consentimiento del afectado titular de dichos datos.

Ahora bien, este consentimiento no será necesario en los siguientes casos:

a) Cuando la cesión esté autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando la comunicación a terceros sea legítima esto es, cuando se limite a la finalidad que la justifica.

d) Cuando la comunicación o cesión de datos tenga como destinatario al Defensor del Pueblo (u órgano autonómico equivalente), al Ministerio Fiscal, a los Jueces o tribunales o al Tribunal de Cuentas (o institución autonómica con funciones análogas), en el ejercicio de sus funciones.

e) Cuando la cesión de datos se dé entre Administraciones Públicas, y tenga como finalidad el tratamiento posterior de estos con fines históricos, estadísticos o científicos.

f) Cuando la cesión lo sea de datos personales relativos a la salud, y sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios de epidemias de acuerdo con la legislación sobre sanidad, ya sea autonómica o estatal.

III. NIVELES DE SEGURIDAD APLICABLES A LOS FICHEROS DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL[13].

1. Niveles de seguridad.

16. A continuación comprobaremos que para analizar cuáles son las medidas de seguridad que debe cumplir la entidad responsable del tratamiento automatizado de los datos de carácter personal es necesario ver previamente cuáles son los niveles de seguridad aplicables a los ficheros de tratamiento de datos de carácter personal.

El RMS clasifica las medidas a aplicar en tres niveles: básico, medio y alto. Dichos niveles, se establecen atendiendo a la naturaleza de la información tratada, en función de la necesidad de garantizar la confidencialidad e integridad de dicha información, esto es, el nivel de seguridad que debe guardar el responsable del fichero viene establecido en función de los datos personales objeto de tratamiento. No obstante, los niveles de seguridad regulados se entenderán como mínimos exigibles sin perjuicio de ulteriores regulaciones y de la aplicación de la legislación específica aplicable en cada materia, que puede exigir medidas adicionales.

El artículo 4 del RMS determina a que tipo de datos corresponde aplicar cada nivel de seguridad. Así, todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de *nivel básico*. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, los ficheros relativos a solvencia patrimonial y crédito y los ficheros que contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo habrán de guardar además de las medidas de nivel básico las de *nivel medio*. Y por último, los ficheros que contengan datos de ideología, religión, creencias, origen

[13] *Vid.* ÁLVAREZ CIVANTOS, Oscar José, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Editorial Comares, Granada, 2001, pp. 113-168.

racial, salud, vida sexual, afiliación sindical así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas, deberán reunir además de las medidas de seguridad de nivel básico y medio, las de *nivel alto*.

En cuanto a los plazos para la aplicación de las medidas de seguridad, el propio RMS estableció en su Disposición transitoria única que, para los sistemas de información que se encontrasen en funcionamiento en el momento de su entrada en vigor, las medidas de nivel básico deberían aplicarse en el plazo de seis meses, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años. Ahora bien, el Real Decreto 195/2000, de 11 de febrero amplió los plazos de la siguiente manera: el plazo máximo para implantar las medidas de seguridad de nivel básico era el 26 de marzo de 2000, conservándose los plazos fijados en el RMS para los niveles medio y alto, esto es, el 26 de junio de 2000 para las medidas de seguridad de nivel medio, y el 26 de junio de 2001 para las de nivel alto. No obstante, en virtud de una Resolución de 22 de junio de 2001 del Ministerio de Justicia que dispone la publicación del Acuerdo de Consejo de Ministros por el que se decidió la ampliación del plazo para la implantación de medidas de seguridad correspondientes al nivel alto hasta el 26 de junio de 2002.

2. Aspectos prácticos en materia de implantación de las medidas de seguridad[14].

17. A efectos prácticos es importante distinguir en función de las medidas de seguridad a aplicar[15]:

1º) Medidas de seguridad de nivel básico:

Las medidas de seguridad de nivel básico son las siguientes:

A) Documento de seguridad (artículo 8 del RMS).

1ª) **"***El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información".*

[14] A estos efectos un modelo de "documento de seguridad" se encuentra en el *cd-rom* que acompaña a este trabajo.
[15] AA.VV., Guía práctica de la Ley Orgánica de Protección de datos, edición en cd-rom, Deloitte & Touche, 2002, pp. 63-85.

Es necesaria la creación de un documento de seguridad que incluya una visión general de las políticas de seguridad que haya definido la entidad para garantizar la protección de los ficheros que contienen datos de carácter personal. Es importante considerar que el documento no debe ser solamente una mera repetición de los aspectos señalados por la ley, sino que este debe reflejar también la situación real existente en la empresa y describir con el máximo detalle posible todas las actividades que se realizan para garantizar la seguridad de los datos de carácter personal. Igualmente es importante que el documento de seguridad sea puesto a disposición del personal de la entidad, para que conozca su contenido y colabore al máximo con la aplicación de las medidas de seguridad.

2ª) *"El documento deberá contener, como mínimo, los siguientes aspectos:*

a) Ámbito de aplicación, especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Documento de Seguridad.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros y descripción de los sistemas de información.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y recuperación de datos".

A la hora de crear el documento de seguridad, es importante tener presente que este debe contener obligatoriamente los aspectos a los que se refiere el artículo 8 del RMS. Cada uno de los aspectos enumerados debe estar definido claramente dentro del documento y en lo posible se evitarán referencias a normas o procedimientos externos.

3ª) *"El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo".*

Es importante que en la entidad exista un equipo responsable de mantener actualizado el documento de seguridad. Para que esto sea posible, es importante reforzar aspectos como la comunicación interna, con el fin lograr que todos los cambios tecnológicos y organizativos sean conocidos por los responsables del mantenimiento del documento y sean debidamente reflejados en él.

4ª) *"El contenido del documento deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal".*

Además de la designación de un equipo responsable del mantenimiento del documento, es importante realizar revisiones periódicas sobre el mismo, con el fin de encontrar continuamente

aspectos de mejora, tanto en la aplicación de las medidas de seguridad, como en la presentación del propio documento. Asimismo, es importante verificar que a pesar de los cambios realizados, el documento contenga todos los requerimientos del reglamento y se aproxime correctamente a la situación real de la empresa.

B) Funciones y obligaciones del personal (artículo 9 del RMS).

1ª) *"Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información, estarán claramente definidas y documentadas de acuerdo a lo establecido en el contenido del documento de seguridad".*

Es importante definir y documentar claramente las funciones y obligaciones del personal, de cara al manejo y tratamiento de los datos de carácter personal, de acuerdo a los derechos y deberes a los que hace referencia la LOPD. Asimismo, las funciones y obligaciones del personal deben actualizarse con cada revisión del documento en función de los cambios producidos a nivel de organización y recursos humanos.

2ª) *"El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten el desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento".*

El personal de la entidad debe conocer en todo momento las implicaciones de sus acciones de cara a la seguridad de los datos afectados por la LOPD. Para esto es conveniente diseñar una política de recursos humanos que esté orientada a la concienciación del personal frente al cumplimiento de la LOPD en el desarrollo de sus funciones diarias y la existencia del Documento de seguridad. Si la entidad desarrolla algún tipo de mecanismo sancionador para el incumplimiento de las medidas establecidas en el documento de seguridad, es importante que sea conocido por el personal de la entidad y que se encuentre en lo posible documentado para que pueda ser difundido fácilmente.

C) Registro de incidencias (artículo 10 del RMS).

1ª) *" El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en el que se ha producido, la persona que realiza la notificación, a quien se le comunica y los efectos que se hubieran derivado de la misma".*

Con el fin de realizar un seguimiento de los efectos de las incidencias notificadas, es importante diseñar procedimientos claros y detallados que puedan servir de guía para lograr una gestión eficiente y controlada de las mismas. Dichos procedimientos deben ajustarse en todo momento a la realidad de la entidad, para lo cual es conveniente que se modifiquen en función a los cambios internos que ocurran sobre los procesos de atención de incidencias. Igualmente, cabe destacar la importancia que tiene la identificación de controles internos que garanticen la aplicación de los procedimientos después de que estos sean definidos. Resulta apropiado recordar que los procedimientos de gestión y notificación de incidencias serán sostenibles en la medida de que sean capaces de adaptarse a la realidad operativa de la empresa. El reto consiste en encontrar procedimientos que se ajusten a la situación real. Solo así se garantizan costes mínimos de aplicación.

D) Identificación y autenticación (artículo 11 del RMS).

1ª) *"El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso".*

Contar con una lista de usuarios facilita las labores de control sobre las personas que tienen accesos autorizados a los sistemas de la entidad, ya que las labores de actualización y mantenimiento permiten analizar la necesidad real que tienen los usuarios de acceder a los sistemas de información de la entidad. Cuando se trata de entidades pequeñas es importante que la lista de usuarios sea incluida en papel dentro del documento de seguridad. Por otra parte, si la obtención de dicha lista se dificulta debido al tamaño del sistema, puede mantenerse almacenada en un fichero o cualquier medio magnético. En este caso el documento de seguridad debe hacer referencia específica a la ubicación del fichero o soporte (indicando su nombre o identificación).

2ª) *"Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad".*

Es importante, que los procedimientos de asignación, distribución y almacenamiento de contraseñas incluyan mecanismos para mitigar los riesgos que se derivan del uso compartido de identificadores de usuarios, y el almacenamiento de las contraseñas en formatos inteligibles. Asimismo, pueden plantearse mecanismos que permitan ocultar las contraseñas cuando estas son tecleadas en la pantalla. Igualmente, y con el fin de garantizar la confidencialidad y la

integridad de las contraseñas deben establecerse en el documento de seguridad, pautas sobre el manejo de contraseñas; Las palabras de paso no deben ser escritas ni almacenadas en ficheros que no sean cifrados, tampoco deben ser divulgadas ni compartidas con otros usuarios. Asimismo, es importante que los permisos de lectura sobre los archivos que contengan contraseñas, sean restringidos únicamente al administrador del sistema.

3ª) *"Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible".*

Si bien el documento de seguridad debe establecer la periodicidad con la que se cambiarán las contraseñas, también es importante que describan los mecanismos existentes para garantizar que las palabras de paso son cambiadas con la periodicidad establecida. En general, todos los sistemas operativos modernos cuentan con la posibilidad de implementar el cambio automático de contraseñas. Es recomendable que se aproveche esta funcionalidad para garantizar que las palabras de paso tienen un tiempo de vida y que no perderán su utilidad debido a un tiempo de uso demasiado prolongado. Asimismo, es importante ofrecer al usuario mecanismos opcionales de cambio de contraseñas en caso de que estos sospechen que su contraseña ha sido descubierta por algún otro usuario.

E) Control de acceso (artículo 12 del RMS).

1ª) *"Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones".*

Con el fin de preservar la intimidad de los individuos, el uso de la información de carácter personal debe ser restringido al máximo, permitiendo el acceso solo a aquellas personas que lo requieran para el desarrollo de sus funciones. La mayoría de los sistemas operativos y muchas aplicaciones, permiten diseñar perfiles de usuario, a través de los cuales es posible restringir para un grupo de usuarios el acceso a ciertos datos. En general, se construirán perfiles de usuario de acuerdo a grupos de personal que cumplan las mismas funciones.

2ª)*"El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados".*

Es conveniente que se realice una revisión periódica de los permisos concedidos a los diferentes usuarios del sistema de información de la entidad. En algunas organizaciones, es frecuente que

el personal cambie de funciones o se desplace a otros departamentos para realizar nuevas funciones. Es frecuente que se habiliten los nuevos permisos sin eliminar los permisos anteriores que ya no le serán requeridos para el desarrollo de sus funciones. Es importante garantizar que los permisos asignados a los usuarios son siempre los que necesita. De esta forma es posible evitar que la información de carácter personal sea utilizada para fines no éticos. Igualmente, es muy fácil implementar un salvapantallas con contraseña que no permita que personal no autorizado utilice las terminales o estaciones de trabajo que han sido dejadas inactivas por otras personas.

3ª) *"La relación de usuarios con acceso autorizado al sistema de información, contendrá el acceso autorizado para cada uno de ellos".*

Es importante que la función de cada persona, corresponda con los accesos que tiene autorizados en el sistema. Una buena manera de controlar esto es mantener una lista autorizadas de usuarios y accesos autorizados. Las tareas de mantenimiento y actualización de dicha lista obligarán a confirmar los accesos autorizados para cada miembro de la lista. Es importante que esta relación de usuarios sea revisada periódicamente para controlas que los accesos están debidamente definidos en el sistema.

4ª) *"Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero".*

Las personas responsables de autorizar los accesos a los datos de carácter personal deben ser conocidas por el personal. Es importante que el personal sea consciente de que ningún usuario debe intentar cambiar los permisos de otros o modificar la configuración de los sistemas. El responsable del fichero debe asignar estas responsabilidades a un grupo de personas específicas que serán identificadas en el documento de seguridad.

F) Gestión de soportes (artículo 13 del RMS).

1ª) *"Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad".*

La identificación apropiada de la información contenida en los soportes permite garantizar la disponibilidad de la información que contienen. En caso de una recuperación de emergencia,

será fácil encontrar los datos necesarios sin perder tiempo. La empresa puede diseñar un sistema de etiquetado de soportes o inventario que permita identificar el soporte y la información que contiene.

2ª) *"La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizado por el responsable del fichero".*

Con el fin de preservar la confidencialidad de los datos de carácter personal, es necesario controlar todas las salidas de soportes. Por este motivo es necesaria la autorización del responsable del fichero. Es recomendable definir y documentar procedimientos de autorización de salida de soportes, que establezcan los modelos de solicitud de autorización y que su aprobación se realice únicamente por escrito.

G) Copias de respaldo y recuperación (artículo 14 del RMS).

1ª) *"El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos".*

En general, las entidades deben contar con procedimientos detallados de copias de seguridad y recuperación de datos con el fin de garantizar la disponibilidad de la información de carácter personal. Es importante que se definan mecanismos para verificar la correcta aplicación de dichos procedimientos. Es posible establecer algunos controles automatizados, como registros de confirmación de copia que permitan establecer que los procedimientos de copias se realizan de la manera correcta.

2ª) *"Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos, deberán garantizar su reconstrucción en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción".*

El responsable del fichero puede establecer recuperaciones periódicas de datos con el fin de verificar que los procedimientos de obtención de copias de respaldo y los respectivos procesos de recuperación, se realizan correctamente. La comprobación de que las copias de seguridad pueden ser cargadas de forma rápida y correcta, permite que el personal responsable de la disponibilidad de la información se familiarice con los procedimientos a seguir en caso de desastre o pérdida de datos. Asimismo, es posible verificar que las copias de seguridad se realizan correctamente y que la información no se corrompe en su almacenamiento.

3ª)" Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos".

El documento de seguridad debe establecer claramente la periodicidad con que se realizan las copias de seguridad. Con el fin de que la entidad pueda garantizar la recuperación total ante algún desastre o fallo en los sistemas, es importante que se realicen copias semanales de la totalidad de los datos. Adicionalmente, pueden programarse copias diarias que incluyan solamente los cambios sobre los datos que se hayan producido durante el día.

2º) Medidas de seguridad de nivel medio:

Las medidas de seguridad de nivel medio son las siguientes:

A) Documento de seguridad (artículo 15 del RMS).

1ª) *"El documento de seguridad deberá contener además de lo dispuesto para el nivel Básico, la identificación del responsable o responsables de seguridad, los controles periódicos que se deben 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".*

Es importante que el personal conozca la identidad de todas las personas que intervienen en la coordinación y el control de las medidas de seguridad, con el fin de que puedan informarles de cualquier anomalía o problema que pueda presentarse en cuanto a la seguridad de los datos de carácter personal.

B) Responsable de seguridad (artículo 16 del RMS).

1ª) *"El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con el reglamento".*

Si bien el responsable del fichero puede ser una persona jurídica, es importante recordar que el responsable de seguridad solo puede ser una persona física. Esta persona estará encargada concretamente de controlar la aplicación de las medidas de seguridad y puede también convertirse un canal de comunicación para que los usuarios de los datos comuniquen posibles

mejoras sobre los sistemas de información, los problemas y las anomalías en todo lo relacionado con la seguridad informática.

C) Auditoría (artículo 17 del RMS).

1ª) *"Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años".*

La realización de la auditoría periódica permite verificar si los controles establecidos a través de las medidas de seguridad son efectivos y si es posible garantizar la integridad, confidencialidad y disponibilidad de los datos de carácter personal. Igualmente, permite garantizar que la empresa cumple con lo establecido por el RMS de cara a una posible inspección de la APD. Es importante que la sociedad realice esfuerzos por detectar la mala aplicación de las medidas o sus deficiencias para poder corregir los problemas relacionados con la seguridad de los datos de carácter personal, y garantizar el cumplimiento de la normativa en todo momento.

2ª) *"El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas".*

El resultado de la auditoría debe reflejarse en un informe final que establezca las debilidades y aspectos susceptibles de mejora, con el fin de que la entidad pueda detectar los problemas a los que se enfrenta en términos de seguridad informática. Mantener documentados los resultados de las auditorías, permite realizar un seguimiento sobre las medidas correctoras que haya que aplicar para corregir las deficiencias detectadas en la auditoría.

3ª) *"Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedaran a disposición de la Agencia de Protección de Datos".*

Con el fin de que las sugerencias y recomendaciones planteadas en el informe de auditoría tengan un impacto positivo sobre la entidad, es importante que sean analizadas e implementadas por el responsable del fichero. Si la auditoría es externa, es conveniente crear un equipo de seguimiento y mejora que se encargue de concretar y evaluar las acciones que se deben adoptar para lograr el cumplimento del RMS o la mejora de la seguridad a nivel general.

D) Identificación y autenticación (artículo 18 del RMS).

1ª) *"El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado".*

Es necesario garantizar que no existe ningún usuario compartido que tenga acceso a los sistemas de información. Igualmente, cuando se trate de acceso de información a través de redes de comunicaciones conviene considerar la aplicación de métodos de autenticación basados en claves públicas o PKI.

2ª) *"Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información".*

El bloqueo de cuentas por reintentos incorrectos permite al administrador tener un control de las cuentas que quedan deshabilitadas temporalmente. Es importante que se revise el registro de las cuentas bloqueadas con el fin de poder detectar los intentos fallidos por vulnerar la seguridad de los sistemas de información de la entidad. Igualmente, restringir el número consecutivo de intentos de acceso fallidos previene la posibilidad de que los usuarios realicen ensayos ilimitados de acceso con el fin de intuir las contraseñas de los usuarios.

E) Control de acceso físico (artículo 19 del RMS).

1ª) *"Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales, donde se encuentran ubicados los sistemas de información con datos de carácter personal".*

A través de la creación de procedimientos de autorización de acceso a las instalaciones en las que se encuentran ubicados los datos de carácter personal, es posible controlar que personas no autorizadas acceden a la información. Igualmente, restringir el acceso a los ordenadores de la empresa fuera del horario de oficina, permite controlar que no se haga uso de los equipos por personal que no esté autorizado para ello. Adicionalmente, mantener el servidor de datos en una habitación separada, cuyo acceso esta restringido al personal que posea llaves, combinaciones o tarjetas, garantiza que los datos estarán protegidos de accesos no autorizados.

F) Gestión de soportes (artículo 20 del RMS).

1ª) *"Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, 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 la recepción que deberá estar debidamente autorizada".*

Es conveniente la creación de procedimientos de entrada de soportes que permitan mantener un registro detallado que incluya la información requerida por el RMS. Es importante determinar las personas que estarán encargadas de crear y mantener el registro, así como los pasos que se deben seguir para autorizar la entrada de soportes a la entidad.

2ª) *"Igualmente se dispondrá de un sistema de registro de salida de soportes informáticos, que permita 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".*

Con el fin de garantizar la confidencialidad de la información personal que trata la empresa, es importante la creación de procedimientos de autorización de salida de soportes que permitan mantener un registro que contenga la información requerida por el RMS.

3ª) *"Cuando un soporte vaya a ser desechado o reutilizado, 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".*

El uso de herramientas de borrado de datos, asegura que la información contenida en un soporte es eliminada físicamente, previniendo recuperaciones no deseadas de los datos protegidos.

4ª) *"Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos".*

Mediante la realización de copias de seguridad antes de cualquier tarea de mantenimiento, se asegura la restauración de todas las modificaciones realizadas sobre los datos personales, en caso de que ocurra un desastre durante la revisión de los equipos. De no ser así se perderían las modificaciones efectuadas desde la fecha de realización de la última copia de seguridad. Igualmente, para garantizar la confidencialidad de los datos es conveniente cifrar los datos que se encuentren en los soportes sobre los que se vayan a realizar las tareas de mantenimiento.

G) Registro de incidencias (artículo 21 del RMS).

1ª) *"En el registro de incidencias, deberán consignarse además, los procedimientos realizados de recuperación de los datos restaurados y en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación".*

Con el fin de garantizar el control sobre la gestión de los procesos de restauración de datos y preservar la integridad y confidencialidad de los mismos, es importante crear un procedimiento específico e independiente de la gestión normal de las incidencias, que permita mantener un registro de las incidencias particulares que involucran procesos de recuperación de datos. Es importante que en este registro se incluyan toda la información requerida por el RMS.

2ª) *"Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos".*

Es conveniente la creación de un formulario de petición de restauración que será cumplimentado por los usuarios con el fin de que el responsable del fichero pueda evaluar la petición y autorizar por escrito la restauración de la información de carácter personal.

H) Pruebas con datos reales (artículo 22 del RMS).

1ª) *"Las pruebas anteriores a la implantación o modificación de los sistemas de Información no se realizarán con datos reales, salvo que se aseguren los niveles de seguridad correspondientes al tipo de fichero tratado".*

La utilización de datos reales en plataformas de test o prueba, implica tanto la declaración de los ficheros ante la APD, como la implantación de las mismas medidas de seguridad aplicadas a los datos reales. De acuerdo a la importancia de las actividades de desarrollo y a la realización de pruebas de volumen, la empresa debe establecer si se utilizarán datos reales para probar las aplicaciones o si, por el contrario está terminantemente prohibido realizar dichas pruebas con datos de personas reales.

3º) Medidas de seguridad de nivel alto:

Las medidas de seguridad de nivel alto son las siguientes:

A) Distribución de soportes (artículo 23 del RMS).

1ª) *"La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte".*

Los soportes que vayan a ser transportados dentro o fuera de la entidad para su distribución deben contener la información cifrada con el fin de que sea posible la preservación de la confidencialidad de los datos. De esta forma se garantiza que solo las personas autorizadas, y que conozcan la clave de descifrado puedan acceder a la información.

B) Registro de accesos (artículo 24 del RMS).

1ª) *"De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado".*

Atendiendo a lo que establece el RMS habrá que prever que de cada acceso se deben guardar estos datos.

2ª) *"En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido".*

De todas las medidas de seguridad exigidas por el RMS, estas son tal vez las más costosas. El almacenamiento de la información de acceso al sistema generalmente consume gran parte de la capacidad de los sistemas de la entidad y reduce el rendimiento. Es importante realizar un análisis técnico que permita definir la mejor manera de aplicar estas medidas.

3ª) *"Los mecanismos que permiten el registro de datos detallados en los puntos anteriores, estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos".*

Es importante controlar que los mecanismos que permiten el registro de accesos no sean desactivados por personas no autorizadas. Es importante que se defina solo una persona responsable de la activación de los registros de acceso, que estará encargada de verificar que los mecanismos de registro se encuentren activados en todo momento.

4ª) *"El período mínimo de conservación de los datos será de dos años".*

Es importante, que la entidad determine, de acuerdo a la configuración técnica que posea, cual es la mejor manera de mantener almacenados los ficheros que contienen los registros de acceso. En general es importante considerar la posibilidad de almacenar los ficheros de registro de acceso en soportes externos, con el fin de no afectar el rendimiento del sistema.

5ª) *"El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes".*

Es importante que el responsable de seguridad, revise periódicamente los registros, con el fin de poder detectar intentos de acceso no autorizados, reiterados y sospechosos. Esta práctica permite mantener un control sobre la seguridad general de los sistemas, protegiendo particularmente la integridad y confidencialidad de la información de carácter personal.

C) Copias de respaldo y recuperación (artículo 25 del RMS).

1ª) *"Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos, en un lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en el reglamento".*

Con el fin de garantizar la disponibilidad de los datos en caso de que ocurra un desastre en la sala donde se encuentran los equipos informáticos, es importante que se almacenen copias de respaldo y los procedimientos de recuperación en un lugar separado. Asimismo, resulta conveniente considerar la adquisición de un armario ignífugo que garantice la integridad de los datos en caso de incendio.

D) Telecomunicaciones (artículo 26 del RMS).

1ª) *"La transmisión de los datos de carácter personal a través de redes de telecomunicaciones de realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros".*

Con el fin de evitar que un posible intrusismo afecte la integridad y confidencialidad de los datos, es importante que cualquier información de carácter personal que viaje a través de las redes de comunicación esté cifrada. Asimismo, para garantizar que la información que viaje a través de redes no sea accedida por terceros es conveniente pensar en la utilización de

procedimientos como la firma electrónica o en la aplicación de métodos de autenticación basados en claves públicas o PKI.

IV. RÉGIMEN JURÍDICO DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL EFECTUADO A TRAVÉS DE INTERNET[16].

1. Consideraciones generales a los tratamientos efectuados a través de Internet.

18. Además de las consideraciones apuntadas hasta ahora en relación con el consentimiento exigido por la LOPD para el tratamiento de datos de carácter personal y las medidas de seguridad aplicables a los ficheros de datos de carácter personal, el tratamiento realizado por las entidades que operan a través de *Internet* presenta una serie de rasgos característicos para el cumplimiento de la normativa sobre protección de datos de carácter personal, que se refieren a la información del afectado y al consentimiento y la forma de prestarlo.

En *Internet* el deber de información que corresponde al responsable del fichero se manifiesta por medio de la política de privacidad que se debe de incluir en un lugar visible del sitio *web*. En dicha política de privacidad el responsable del fichero deberá, para cumplir con lo previsto en el artículo 5 de la LOPD, informar a los afectados a los que se soliciten datos de carácter personal de modo expreso, preciso e inequívoco:

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

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

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

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

[16] *Vid.* ÁLVAREZ CIVANTOS, Oscar José, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Editorial Comares, Granada, 2001, pp. 230-243.

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

En la práctica la gran mayoría de los sitios *web* incluyen una dirección de correo electrónico específica para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, aunque, esto nos plantea problemas de aplicación en Internet, ya que la APD en la Instrucción 1/1998, de 19 de enero, estableció como necesario, a los fines de poder constatar la identidad de la persona que solicita el acceso a sus datos, el que aporte o remita una copia del D.N.I.

Por otro lado, el responsable del fichero debería dejar constancia en su política de privacidad de los siguientes aspectos:

- De su Política en cuanto a la cesión o no de los datos a terceras personas y de la solicitud de al afectado de su consentimiento para tal menester.

- De la destrucción de los datos almacenados para el caso de extinción de la entidad responsable del fichero.

- De las cláusulas que aclaren como debe realizar el afectado la prestación de su consentimiento para la recogida de sus datos de carácter personal.

- Del uso de mecanismos complementarios de recogida de datos o información de sus visitas, como, por ejemplo, pude ser la efectuada por medio de las *cookies*.

- De las cláusulas eximentes de responsabilidad por el tratamiento de datos que efectúen otros sitios *web* a las que pueda acceder desde la del responsable del ficheros al cliquear sobre un link, un *banner* o sobre cualquier otro enlace ubicado en la *web* con esta finalidad.

- De las cláusulas que determinen el plazo de vigencia de la política de privacidad y de la forma en que se habrá de producir y comunicar el cambio de la misma.

- De la mención de los derechos de los menores en el tratamiento de sus datos de carácter personal y de la necesidad de que el consentimiento para que el mismo sea concedido por sus padres o tutores.

2. La protección de datos de carácter personal y el uso de las *cookies*.

19. La defensa del derecho a la intimidad frente al uso de las nuevas tecnologías encuentra su mayor razón de ser en *Internet* y, en concreto, con el uso de las denominadas *cookies*. La función de estos archivos es la de registrar las visitas que el usuario hace a un determinado sitio *web*; si una misma empresa se encarga de transferir *cookies* a los visitantes de los sitios *web*, ésta puede recoger una valiosa información acerca de qué sitios *web* son más visitados por ese usuario, permitiéndole crear perfiles de los usuarios de la red.

La función básica de las *cookies* consiste en permitirle a un servidor almacenar y más adelante recuperar una pequeña cantidad de información en el ordenador del usuario. Estos datos siempre estarán asociados a un sitio *web* y a un navegador concreto, lo que implica que una *cookie* creada por un servidor en un momento dado sólo le será accesible en el futuro si el visitante regresa a ese sitio *web* usando el mismo ordenador y el mismo navegador. La información es guardada en un archivo de texto, conteniendo sólo aquellos datos que la aplicación servidora expresamente determine. Aunque puede incluir alguna información personal, como códigos de usuario o contraseñas, lo normal es recoger sólo aquellos datos que permitan recordar lo que el usuario hizo en esa ocasión. En el momento en que el usuario en cuestión regresa a ese sitio *web* en cuestión, su navegador envía el contenido de la *cookie* al servidor, que puede entonces interpretarlo y usarlo de un modo preestablecido, para, por ejemplo, mostrar un saludo personalizado al usuario.

Frente al uso de las *cookies*, es cierto que se han diseñado programas *anticookies* e incluso la mayoría de los navegadores permiten al usuario elegir una opción que impedirá el almacenamiento de *cookies* en su ordenador pero, no es menos cierto que existen determinados sitios *web* cuyo acceso es imposible si no se acepta la instalación de las mismas en el disco duro del ordenador que accede a un determinado sitio *web*.

Ahora bien, en relación con la defensa del derecho a la intimidad y la protección de datos de carácter personal, y el uso de las *cookies*, debemos hacer algunas precisiones: primero, las *cookies* no pueden capturar información personal de un usuario que no esté dispuesto a cederla voluntariamente; segundo, no pueden transmitir un virus informático porque no contienen más que un texto estático; tercero, no pueden entrar en el disco duro del ordenador del usuario y extraer documentos u otros archivos; y, cuarto, la utilización de esta técnica no vulnerará el derecho a la intimidad, el derecho a la protección de datos y, por ende, la LOPD, cuando se haga con el consentimiento del usuario.

3. El establecimiento de una política de protección de datos de carácter personal.

20. Como hemos apuntado anteriormente, todo aquel que pueda tratar datos de carácter personal, debe informar acerca de su política de privacidad de datos de carácter personal.

En particular y atendiendo a lo anteriormente expuesto, recomendamos que en toda política de privacidad de las siguientes cuestiones:

a) Recopilación de la información personal.

b) Uso de la información personal.

c) Seguridad de la información personal.

d) Uso de las *cookies*.

e) Cesión de datos a terceros.

f) Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

g) Cumplimiento de su Política de Privacidad de Datos de Carácter Personal.

h) Modificación de su Política de Privacidad de Datos de Carácter Personal.

CAPÍTULO SEGUNDO
INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS Y RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS

I. INFRACCIÓN DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL[17].

21. Por último, tras unas breves consideraciones preliminares, vamos a estudiar el procedimiento sancionador por infracción de las normas sobre protección de datos de carácter personal, en el que se puede ver inmerso todo aquel que vulnere las normas protectoras de los datos de carácter personal.

1. Tipos de infracciones.

La LOPD, siguiendo una buena técnica legislativa, no ha tipificado ningún tipo de delito sino que ha remitido a sus sedes jurisdiccionales respectivas, penal y civil, las sanciones correspondientes a ambos tipos de responsabilidades. Así pues, quien se crea perjudicado en sus intereses por una actuación ilícita en el ámbito de la protección de datos de carácter personal y, pueda demostrar que se le ha causado un daño podrá presentar la correspondiente demanda ante la jurisdicción civil solicitando una indemnización por daños y perjuicios. De igual forma, la vulneración del derecho a la intimidad en sus aspectos más graves se remite a la sede penal y, así, es en el Código Penal donde figuran tipificados este tipo de delitos.

La LOPD sólo contempla sanciones administrativas que se convierten en multas en el caso de los ficheros privados y en propuestas de sanciones disciplinarias en el caso de los ficheros públicos. Estarán sujetos al régimen sancionador establecido en la LOPD los responsables de los ficheros o responsables de los tratamientos y los encargados de los tratamientos.

Además, la LOPD sujeta a los responsables del fichero y a los encargados del tratamiento al régimen sancionador establecido en el Título VII de la misma. El artículo 44 de la citada Ley establece las conductas que son consideradas como infracción, en los siguientes términos:

1) Infracciones leves:

Según el artículo 44.2 de la LOPD, son infracciones leves las siguientes:

[17] *Vid.* ÁLVAREZ CIVANTOS, Oscar José, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Editorial Comares, Granada, 2001, pp. 245-252.

"a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda."

Se infringe en este caso el artículo 16 de la LOPD que obliga al responsable del tratamiento a hacer efectivo este derecho en el plazo de diez días.

"b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos."

Es función de la Agencia de Protección de Datos, según establece el artículo 37.i) de la LOPD, recabar de los responsables de los ficheros o de los tratamientos cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

"c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave."

Según el artículo 26 de la LOPD, *"toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo debe notificar previamente a la Agencia de Protección de Datos"*.

"d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley."

Según el artículo 5 de la LOPD los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de una serie de circunstancias sobre el fichero, previéndose en dicho artículo una serie de excepciones.

"e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave."

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

2) Infracciones graves:

Son infracciones graves, según el artículo 44.3 de la LOPD, las siguientes:

"a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal par los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado o Diario oficial correspondiente."

Según el artículo 20 de la LOPD, *"la creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente".*

"b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad."

Uno de los principios en que se inspira la LOPD es el de finalidad por el que, como establece el artículo 4.1 de la LOPD, *"los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".*

"c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los que éste sea exigible."

El artículo 6 de la LOPD ordena, salvo en una serie de casos que figuran como excepciones, recabar el consentimiento inequívoco como trámite previo al tratamiento de los datos de carácter personal.

"d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave."

Se trata de un precepto de carácter muy general referido a la fase de tratamiento de los datos.

"e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada."

El artículo 15 de la LOPD otorga al afectado la posibilidad de solicitar y obtener información sobre sus datos de carácter personal que figuren en los ficheros; asimismo según el artículo 30

de la LOPD tendrán derecho a oponerse al tratamiento de sus datos con fines de publicidad y de prospección comercial.

"f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara."

Según el artículo 16 de la LOPD, "el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días".

"g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo."

La vulneración del deber de secreto que ya se contemplaba como falta leve en este caso se agrava cuando se refiere a un determinado tipo de ficheros que recogen los datos que vienen a continuación:

1. Comisión de infracciones administrativas o penales.
2. Hacienda Pública.
3. Servicios financieros.
4. Prestación de servicios de solvencia patrimonial y crédito.
5. Conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

"h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen."

La seguridad en general a la que se refiere el artículo 9 de la LOPD es uno de los pilares sobre los que se ha de cimentar la protección que otorga la Ley, pues sin ella prácticamente nada se puede garantizar.

"i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos."

La Agencia de Protección de Datos tienen entre sus funciones, según establece el artículo 37.i) de la LOPD, la de *"recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones"*.

"j) La obstrucción al ejercicio de la función inspectora."

Una de las potestades que la Ley concede al Director de la Agencia de Protección de Datos es la potestad inspectora. Así, como establece el artículo 40 de la LOPD, *"las autoridades de control podrán inspeccionar los ficheros que contengan datos de carácter personal recabando cuantas informaciones precisen para el cumplimiento de sus cometidos"*.

"k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos."

La obligación de notificar a la Agencia de Protección de Datos la creación de un fichero viene dada en el artículo 26.1 de la LOPD, procediendo el Registro General de Protección de Datos a la inscripción del fichero cuando la notificación se ajuste a los requisitos exigibles.

"l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado."

Según el artículo 5.4 de la LOPD, *"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"*.

3) Infracciones muy graves:

Según el artículo 44.4 de la LOPD son infracciones muy graves las siguientes:

"a) La recogida de datos en forma engañosa y fraudulenta."

El artículo 4.7 de la LOPD prohíbe la recogida de datos cuando ésta se efectúa por medios desleales, fraudulentos o ilícitos.

"b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidos."

La comunicación o cesión de datos a un tercero sin consentimiento del interesado deja a éste indefenso y puede vulnerar lo dispuesto en el artículo 4.2 de la LOPD.

"c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado, recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7."

El tratamiento de datos especialmente protegidos, sin las debidas garantías para el afectado, es lógico que sea sancionado con dureza por las especiales características de dichos datos en relación con la intimidad de la persona y el perjuicio que su conocimiento por terceros sin su consentimiento puede suponer.

"d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso."

Si se efectúa el tratamiento de datos de carácter personal de forma ilegítima, los afectados pueden solicitar del responsable del fichero que cese en este tratamiento, pudiendo reclamar ante el Director de la Agencia de Protección de Datos en caso de no ser atendidos.

"e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos."

La transferencia de datos a un país que no garantice unas condiciones mínimas de protección deja al afectado totalmente desprotegido respecto a cómo van a ser utilizados sus datos de carácter personal y con qué finalidad; por ello es necesario tomar toda esta serie de cautelas.

"f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales."

La referencia a los derechos fundamentales que aquí hace el legislador parece redundante pues los derechos a los que puede afectar son los que protege precisamente la propia LOPD.

"g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas."

Se comete una infracción muy grave de las previstas en la LOPD cuando se vulnera el deber de guardar secreto sobre los datos correspondientes a ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, así como, los datos de carácter personal recabados para fines policiales, siempre y cuando no exista consentimiento de la persona afectada.

"h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición."

La reiteración en la no atención u obstaculización en el ejercicio de los derechos de acceso, rectificación, cancelación u oposición agrava la infracción que ya figuraba como grave en la propia LOPD.

"i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero."

La reiteración en la falta de notificación de la inclusión de datos de carácter personal en un fichero agravará la infracción que ya figuraba en la propia LOPD.

2. Tipos de sanciones.

22. Las sanciones que puede imponer la APD, en el ejercicio de sus funciones se recogen en el artículo 45 de la LOPD y se dividen, tal y como corresponde a las infracciones, en leves, graves y muy graves.

Según establece el artículo 45.4 de la LOPD, *"la cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, el volumen de los tratamientos afectados, 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"*.

Según establece el propio artículo 45 de la LOPD, *"las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas"*, *"las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas"* y, *"las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas"*. Ahora bien, como

establece el artículo 45.7 de la citada Ley, *"el Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios"*.

Además, el artículo 46 de la LOPD regula el procedimiento sancionador en el caso de que las infracciones que señala el artículo 44 se cometan en ficheros de los que sean responsables las Administraciones Públicas.

Ante una infracción de este tipo, el Director de la APD dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

Según establece el artículo 46.2 de la LOPD, *"el Director de la Agencia de Protección de Datos podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran"* y, *"el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas"*.

Además, *"se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieran los apartados anteriores"*, según señala el artículo 46.3 de la LOPD.

Según el artículo 46.4 de la LOPD, *"el Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores"*.

El plazo de prescripción de las infracciones, establecido por la LOPD en su artículo 47, es de tres años para las infracciones muy graves, dos para las graves y un año para las leves. Este plazo comienza a contarse en el momento de comisión de la infracción y la prescripción quedará interrumpida cuando el interesado tenga conocimiento del procedimiento sancionador, reanudándose únicamente si el expediente sancionador estuviere paralizado por un plazo superior a seis meses por causas no imputables al presunto infractor.

El citado artículo 47 de la LOPD establece también el plazo de prescripción de las sanciones que será de tres años para las impuestas por faltas muy graves, de dos para las impuestas por faltas graves y de un año para las impuestas por faltas leves. El plazo de prescripción de las sanciones comienza a contarse desde el día siguiente a aquel en que adquiere firmeza la resolución que impone la sanción, y se interrumpirá por la iniciación con conocimiento del interesado del procedimiento de ejecución, volviendo a transcurrir si el mismo se paraliza por plazo superior a seis meses por causa no imputable al infractor.

3. El procedimiento sancionador.

23. El artículo 48 de la LOPD establece que el procedimiento sancionador se establecerá por vía reglamentaria, correspondiendo a la APD la competencia sobre el mismo. En la medida en que no existe desarrollo reglamentario posterior a la entrada en vigor de la LOPD, la misma establece en su Disposición transitoria tercera la vigencia del Real Decreto 1332/1994 de desarrollo de la LORTAD.

El procedimiento sancionador se iniciará mediante acuerdo de la APD. Siempre de oficio, por propia iniciativa o bien por denuncia de cualquier persona afectada por la conducta del responsable del fichero. En dicho acuerdo la APD designará un instructor[18] y un secretario, identificándose a la persona o personas presuntamente responsables con concreción de los hechos que se le imputen, infracción a la que dan lugar y sanción que le corresponda, pudiendo incluirse en la misma, la adopción de medidas provisionales.

Dentro de los quince días siguientes a la notificación del acuerdo de incoación del expediente, el instructor ordenará de oficio la práctica de cuantas pruebas y actos de instrucción sean adecuados para esclarecer los hechos y determinar las responsabilidades susceptibles de sanción. En idéntico plazo, el presunto responsable podrá formular las alegaciones y proponer las pruebas que considere convenientes.

Transcurrido este último plazo, el instructor acordará la práctica de las pruebas que estime pertinentes, a cuyo efecto concederá un plazo de treinta días, transcurrido el cual el expediente se pondrá a disposición del presunto responsable para que, en el plazo de quince días, formule nuevas alegaciones y aporte la documentación que estime de interés en su defensa.

Finalizada la función instructora, el instructor formulará propuesta de resolución motivada en la que se incluirá la infracción y sanción a imponer y en cuantía de acuerdo a los criterios marcados en la LOPD, notificándola al presunto responsable para que en el plazo de 15 días pueda formular nuevas alegaciones si lo estima oportuno. Finalizado este plazo, la propuesta y el expediente se elevarán al Director de la Agencia de Protección de Datos, que antes de dictar resolución podrá proponer que se lleven a cabo cuantas actuaciones considere necesarias en plazo de quince días. En los diez días siguientes a la expiración de este último plazo el Director de la Agencia de Protección de Datos dictará resolución precisando los hechos imputados, la infracción cometida y precepto en el que se incluye, el responsable de la misma y la sanción impuesta, además de las medidas provisionales que considere oportunas. Esta resolución agota la vía administrativa y contra la misma se podrá interponer recurso contencioso-administrativo.

[18] La función instructora compete a la Inspección de Datos, órgano de la Agencia de Protección de Datos, al cual se atribuyen las funciones de inspección de acuerdo con los artículos 27 y ss. del Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la Agencia de Protección de Datos.

Además, según establece el artículo 49 de la LOPD, *"en los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos"*.

En este sentido, como establece el citado artículo 49 de la LOPD, *"si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas"*.

II. RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN.

24. La responsabilidad de un prestador de servicios de la "Sociedad de la Información", según establece la reciente LSSI, depende de la actividad que realice el prestador de servicios: a) la realización de copias temporales de los datos solicitados por los usuarios; o, b) el alojamiento o almacenamiento de datos.

1. Responsabilidad de los prestadores de servicios que realicen una copia temporal de los datos de carácter personal solicitados por los usuarios.

Establece el artículo 15 de la LSSI que *los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio, y con la única finalidad de hacer más eficaz su transmisión a otros destinatarios que lo soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de estos datos ni por la reproducción temporal de los mismos, si:*

a) No modifican la información.

b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y

e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.

2º Que se ha imposibilitado el acceso a ella, o

3º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

2. Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos de carácter personal.

Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, según el artículo 16 de la LSSI, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

En este sentido, se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el artículo 16.1.a) de la LSSI *cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.*

Además, *la exención de responsabilidad establecida en el artículo 16.1 de la LSSI no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.*

CAPÍTULO TERCERO
TRANSFERENCIA INTERNACIONAL DE DATOS

I. LA TRANSFERENCIA INTERNACIONAL DE DATOS EN LA LOPD[19].

1. Concepto de transferencia internacional de datos.

25. La transferencia internacional de datos personales de un Estado a otro es tema de especial atención en las Leyes de protección de datos. Todos los principios y derechos recogidos en las mismas se ven seriamente amenazados si no se establece un control que marque unos límites de garantía y seguridad en la transmisión telemática o en la transferencia de los datos personales cruzando fronteras. Por ello, la regulación de los límites a la transferencia de datos se encuentra, a nuestro juicio, en el origen de las normas nacionales e internacionales reguladoras de la protección de datos. Precisamente, las normas internacionales que regulan la materia tienen por objeto establecer un núcleo básico de principios de protección de datos que permita considerar uniforme el régimen aplicable en los Estados signatarios, permitiendo así el flujo de información hacia los mismos e impidiendo su transmisión a quienes no cumplan esos principios[20].

26. La transferencia internacional de datos de carácter personal es una de las actividades que regula con más cautela la LOPD con el objeto de prohibir las exportaciones de datos de carácter personal cuando se compruebe previamente que el lugar de destino no ofrece una protección semejante a la otorgada en la UE[21]. En la medida en que el movimiento internacional de datos es libre entre los países de la UE, sólo existe una transferencia internacional de datos cuando el país de destino sea un tercer Estado, esto es, un Estado no miembro de la UE. No puede hacerse ninguna exportación de datos a países terceros, desde España, salvo que se hayan declarado, como destinos seguros por el Ministerio de Justicia o se haya obtenido previamente una autorización de la APD.

27. Sin embargo, esa transmisión debe efectuarse de tal modo que los derechos de los particulares a quienes los datos se refieren y, en especial, su intimidad, queden plenamente garantizados. De ahí que la Exposición de Motivos de la Directiva 95/46/CE recuerde, en su considerando 7, la necesidad de conciliar la protección de los derechos de los ciudadanos en los

[19] *Vid.* AA.VV., Guía práctica de la Ley Orgánica de Protección de datos, edición en cd-rom, Deloitte & Touche, 2002, pp. 46-62.

[20] En este sentido, no debemos olvidar que las transferencias internacionales de datos de carácter personal están al orden del día; así, por ejemplo, se ha calculado que en vuelo del Boeing-747 requiere la transmisión de alrededor de 27.000 mensajes relativos a reservas de billetes y, que American Express maneja más de 1.000.000 de FID diarios en transacciones crediticias.

[21] Consecuentemente, las Órdenes del Ministerio de Justicia de 2 de febrero de 1995 y de 31 de julio de 1998, realizan una "Lista blanca" de países respecto de los cuales se reconoce que otorgan una protección equivalente.

Estados Miembros, a fin de que las garantías que dicha protección establezca no puedan "*constituir un obstáculo para el ejercicio de una serie de actividades a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario"*. Por tanto, el régimen regulador de las transferencias internacionales de datos trata de conciliar la circulación de la información sobre las personas con los derechos de los afectados, logrando un equilibrio en ocasiones sumamente complejo, como complicado puede resultar, en ocasiones, el entendimiento de las normas que lo integran.

28. La norma primera de la Instrucción 1/2000, de 1 de diciembre, de la APD, relativa a las normas por las que se rigen los movimientos internacionales de datos, define la transferencia internacional de datos como "toda transmisión de los mismos fuera del territorio español". Tomando en consideración este concepto, debe indicarse que, tal y como indica la Memoria de la APD correspondiente a 1999, el fundamento de las transferencias internacionales de datos cuya inscripción ha sido solicitada en el RGPD se encuentra básicamente, en dos causas esenciales: a) Por una parte, en la necesidad de armonización y puesta en común de los sistemas de información de los grupos empresariales. Así sucede en los casos en que la gestión de personal, clientes y proveedores o actividad de un determinado grupo se centraliza en los sistemas de la sociedad matriz, con la finalidad de crear estrategias uniformes; y, b) Por otra parte, las transferencias pueden tener por objeto la prestación de un mejor servicio a los clientes del responsable del fichero. Así sucedería en el caso de prestación al cliente de servicios cuando éste se encuentre en un país distinto al de su residencia habitual.

29. A tenor de la Instrucción 1/2000, de 1 de diciembre de 2000, de la APD antes mencionada, se considera movimiento internacional de datos *"toda transmisión de los mismos fuera del territorio español"* y, en particular, *"se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero"*.

El régimen a que se someten los movimientos internacionales de datos de carácter personal se establece en los artículos 33 y 34 de la LOPD. En este sentido, en el artículo 33.1 de la LOPD, se establece que *"no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas"*.

30. La necesidad de conciliar los derechos de los ciudadanos con el movimiento internacional de datos obliga a que las normas reguladoras de la materia partan de un principio general de prohibición de la transferencia a terceros estados que no garanticen un nivel de protección adecuado. Ello supone que, en principio, y sin perjuicio de la existencia de supuestos excepcionales la transferencia queda vedada a empresas situadas en terceros Estados cuya regulación no reconozca el núcleo básico de principios de protección de datos al que nos referimos con anterioridad.

31. La primera cuestión a plantear será, en consecuencia, la de determinar cuándo un tercer estado ofrece un nivel de protección "*adecuado*", esto es, cuándo se considera que su regulación incorpora ese núcleo esencial de principios de protección de datos. La Directiva 95/46/CEE ofrece una solución a la cuestión en su artículo 25.2, que reproduce, en lo esencial, el artículo 33.2 de la LOPD, al señalar que "*el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países*.". Este precepto se verá complementado por el artículo 25.4 de la Directiva 95/46/CEE, según el cual, siempre se considerará que ofrecen un nivel de protección adecuado aquellos terceros Estados respecto de los cuales la Comisión Europea haya declarado la existencia de esa adecuación, lo que también contempla el artículo 34 k) de la LOPD, cuando afirma que no será necesaria autorización del Director de la APD "*cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza* un *nivel de protección adecuado*".

32. En consecuencia, sólo serán, en principio, válidas las transferencias efectuadas a los Estados Miembros de la UE y a los Estados cuya adecuación haya sido declarada por la Comisión Europea. Hasta la fecha, sólo se considerarían adecuados los regímenes de los Estados integrantes del Espacio Económico Europeo (Islandia, Noruega y Liechtenstein) y los afectados por las Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/CE, de 26 de julio (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como de los EE.UU. y Canadá.

33. Finalmente, merece la pena señalar que, a tenor del artículo 12 de la LOPD, cuando la transferencia internacional de datos tenga su fundamento en la *"realización de un tratamiento de datos por cuenta del responsable del fichero"*, los términos en los que se desarrollará el servicio constarán por escrito.

2. Excepciones: régimen de autorización de las transferencias internacionales de datos.

34. No obstante, no se permiten transferencias de datos *"a países que no proporcionen un nivel de protección equiparable"* al que ofrece la LOPD, salvo que el transmitente cumpla lo previsto en la LOPD y el Director de la LOPD autorice la transmisión *"si se obtienen las garantías adecuadas"*; así, en el artículo 34 de la LOPD se recogen toda una serie de excepciones en esta materia:

"a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
e) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de Servicios sanitarios.
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la ejecución da un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.
Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".

Cuando el movimiento internacional de datos se realice bajo el amparo de alguno de los apartados a) a j) del artículo 34 de la LOPD, la APD podrá requerir al responsable del fichero, *"que aporte la documentación que justifique su alegación"*, en el caso de destinatarios situados en países que no pertenecen a la UE ni al Espacio Económico Europeo, respecto de los cuáles la Comisión Europea no haya declarado que existe un nivel adecuado de protección. Y, cuando la transferencia internacional de datos se base en el supuesto k) del artículo 34 de la LOPD, será el Director de la APD quién debe autorizarla. La autorización de la transferencia por la APD se otorgará cuando el *"responsable del fichero aporte un contrato escrito, celebrado entre el transmitente y el destinatario, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos"*.

35. El régimen general de prohibición de la transferencia a terceros estados que no otorguen un nivel adecuado de protección es objeto de una larga serie de excepciones, contenidas en los artículos 33 y 34 de la LOPD, que traen su causa de lo establecido en los artículos 25 y 26 de la Directiva 95/46/CE. Por tanto, dichas excepciones responden a un doble criterio: a) Atienden a las circunstancias concurrentes en el caso concreto que motiva la transferencia (artículo 34 de la LOPD); b) Se fundan en la autorización singular del Director de la APD (artículo 33.1 *in fine* de la LOPD).

A) En cuanto a las primeras, siguiendo la clasificación contenida en el artículo 26.1 de la Directiva 95/46/CEE, pueden fundarse en seis causas esenciales:

1ª) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista, a tenor del artículo 34.e) de la LOPD.

2ª) Cuando la transferencia se encuentre directamente relacionada con la celebración de un contrato en que sea parte el afectado. En este supuesto cabe incluir dos de las excepciones enumeradas por la LOPD: a) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado, a tenor del artículo 34.f) de la LOPD; y, b) Cuando se refiera a transferencias dinerarias conforme a su legislación específica, a tenor del artículo 34.d) de la LOPD.

3ª) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero, en virtud del artículo 34.g) de la LOPD.

4ª) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios, en virtud del artículo 34.c) de la LOPD.

5ª) Cuando la transferencia se funde en un interés público. En este caso cabría hacer referencia a los siguientes supuestos: a) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, según establece el artículo 34.i) de la LOPD; b) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias, a tenor del artículo 34.h) de la LOPD; c) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España, a tenor del artículo 34.a) de la LOPD; y, d) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional, a tenor del artículo 34.b) de la LOPD.

6ª) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo, según establece el artículo 34. j) de la LOPD.

B) En caso de no concurrir uno de los supuestos singulares a los que acabamos de hacer referencia, la transferencia aún será posible, siempre y cuando la misma sea debidamente autorizada por el Director de la APD.

En este sentido, el artículo 33.1 de la Ley, tras establecer la regla general de prohibición a la que nos referimos en un momento anterior, añade que será posible la transferencia en los supuestos en que *"además de haberse observado lo dispuesto en ésta*[22]*, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas"*.

Es decir, en aquellos supuestos en que la transferencia no se funde en la existencia en el país de destino de un adecuado nivel de protección o quepa amparar la misma en un supuesto taxativamente enumerado en la Ley, aún será posible la transmisión de los datos si la remitente y la destinataria de los datos adoptan una serie de medidas que, a juicio del Director de la APD, suplan la inseguridad que pudiera existir en el lugar de destino de los datos.

[22] Nos estamos refiriendo a la mencionada LOPD.

3. Actividad de la APD en materia de transferencia internacional de datos.

36. De lo hasta ahora comentado, cabe deducir que las normas reguladoras de las transferencias internacionales de datos establecen un sistema sumamente complicado de reglas generales y excepciones, basadas en el derecho interno y en el derecho comunitario, que era necesario precisar. Por este motivo, y con la intención de dar cumplimiento a las decisiones de la Comisión Europea adoptadas en este ámbito, la APD adoptó, el 1 de diciembre de 2000, una Instrucción[23] en que, con una finalidad esencialmente orientativa, se establecen los criterios seguidos por la APD, de conformidad con la LOPD y las previsiones de la Directiva, en este ámbito.

37. Así, el apartado primero del Preámbulo de la Instrucción indica que "*la presente Instrucción tiene por objeto señalar los criterios orientativos seguidos por la Agencia de Protección de Datos en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que, en uso de las competencias que la Ley le atribuye, se sigue por la Agencia en cada caso concreto*". Por ello, concluye*, "no es finalidad de esta Instrucción efectuar innovación alguna dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido por la Agencia para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos"*.

38. La Instrucción se compone de 6 normas, divididas en dos secciones, referida la primera a los criterios aplicables a cualquier transferencia internacional de datos y la segunda a supuestos concretos de transferencia. A continuación, trataremos de exponer, con la mayor claridad posible, el contenido de la Instrucción, atendiendo fundamentalmente a la estructura de la misma.

A) Ámbito de aplicación de la Instrucción.

Según se indica en la Norma primera, la Instrucción resultará de aplicación a cualquier supuesto de transferencia internacional de datos, esto es, a cualquier actividad que suponga la transmisión de datos de carácter personal "*fuera del territorio español*".

[23] Instrucción 1/2000, de 1 de diciembre de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

A continuación, la citada Norma diferencia dos supuestos concretos de transferencia, al indicar que "*en particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero"*.Ello supone que a efectos de la aplicación de las normas reguladoras de las transferencias internacionales de datos carece de relevancia el hecho de que la entidad destinataria de los datos utilice los mismos en su propio beneficio o únicamente para realizar una actividad complementaria de la efectuada por la entidad española que transmite los datos, dado que las normas que regulan las transferencias tiene por objeto evitar los perjuicios que pueden derivarse de la salida de los datos a territorio de terceros Estados, siendo éstos similares en uno u otro caso[24].

B) Aplicación de los principios de protección de datos de la LOPD.

La Norma segunda de la Instrucción contiene un principio esencial que, como indica el apartado segundo de su Preámbulo, gobierna todo el régimen regulador de transferencias internacionales. Según indica este principio, contenido en el artículo 25.1 de la Directiva 95/46/CEE, "*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*". Por ello, y con independencia del supuesto de transferencia ante el que nos encontremos, la recogida y tratamiento de los datos en España deberá respetar en su integridad los principios contenidos en la Ley, debiendo obtenerse el consentimiento del afectado salvo cuando la LOPD permita el tratamiento inconsentido de los datos (artículo 6 de la LOPD), siendo el consentimiento expreso en los casos que prevé la Ley (artículo 7 de la LOPD) informando al interesado del tratamiento, su finalidad, destinatarios de los datos y posibilidad de ejercitar sus derechos (artículo 5 de la LOPD), ajustándose a los principios de calidad de datos y finalidad, sin que los datos puedan utilizarse para fines incompatibles con los que motivan su recogida (artículo 4 de la LOPD), imponiéndose al responsable del fichero los deberes de seguridad (artículo 9 de la LOPD) y secreto profesional (artículo10 de la LOPD) y permitiendo a los interesados ejercitar sus derechos, en los términos que la LOPD establece.

C) Deberes formales del transmitente de los datos.

[24] En consecuencia, las medidas que nuestra LOPD prevé serán igualmente aplicables a supuestos en que exista una venta de datos y aquellos otros en los que los datos simplemente se encuentren alojados en un servidor situado fuera de España.

La Norma tercera de la Instrucción desarrolla el modo en que deberá darse cumplimiento a la obligación de notificar la transferencia internacional de datos al RGPD, integrado en la APD.

En cuanto al procedimiento para el cumplimiento de este deber, la Instrucción establece las siguientes reglas:

- La notificación de la transferencia se efectuará en los términos que se contengan en el modelo normalizado aprobado a tal efecto por el Director de la APD, con expresa indicación del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la citada LOPD, para no recabar la autorización expresa del Director de la APD.

- Recibida la notificación, la APD podrá requerir al responsable del fichero para que en el plazo de diez días aporte la documentación necesaria para completar la información relativa a la trasferencia internacional contenida en aquélla, así como la identidad del receptor de la misma. En particular podrá solicitar que se acredite la existencia de consentimiento o relación contractual que habilite la transferencia.

- Al requerirse la información a la que se refiere este apartado se indicará al responsable del fichero que, en caso de no ser aquélla aportada en el plazo de diez días, se le tendrá por desistido de su petición de inscripción o modificación, archivándose ésta.

- Si con la documentación aportada no se acreditara el cumplimiento de los requisitos contenidos en la LOPD, el Director de la APD, en ejercicio de las competencias que le atribuye dicha LOPD, denegará la Inscripción o su modificación.

La denegación así producida surtirá un importante efecto, dado que la inscripción del fichero en el RGPD es requisito previo y necesario para que el tratamiento de los datos de carácter personal pueda entenderse realizado de conformidad con lo establecido en la Ley. Por ello, la realización de una transferencia internacional no inscrita debidamente en el RGPD podría dar lugar a la imposición de una sanción en materia de protección de datos, siendo esta muy grave cuando los datos sean transferidos "*con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos*".

D) Normas especiales atendiendo al país de destino de los datos.

En virtud de las Normas cuarta y quinta, podemos distinguir los siguientes supuestos:

1) Transferencia a Estados Miembros de la Unión Europea o del Espacio Económico Europeo.

La Ley no prevé especialidades respecto de estos países, excluidos de cualquier autorización del Director de la APD por su artículo 34.k) de la LOPD. Por este motivo, únicamente será necesario el cumplimiento de las disposiciones de la Ley en la recogida y tratamiento previos a la transferencia y la notificación de la misma al RGPD.

2) Transferencia a países respecto de los que se haya declarado un nivel adecuado de protección.

Como regla general rige un efecto similar al indicado en el epígrafe anterior. No obstante la Instrucción, atendido lo establecido en las Decisiones de la Comisión Europea por las que se declara la adecuación de Suiza, Hungría y entidades de los EE.UU.[25] y Canadá[26], adheridas a los denominados "*principios de Puerto Seguro*", establece dos precisiones, una general y otra referida al último de los supuestos citados.

En cuanto a la previsión general, se prevé la posibilidad de que el Director de la APD pueda impedir una transferencia concreta o suspender una serie sucesiva de transferencias a estos países en caso de que la destinataria de los datos haya incumplido su Ley nacional o existan indicios de dicho incumplimiento y la autoridad del Estado destinatario no adopte medidas para impedirlo, causando un perjuicio a los afectados.

Por lo que respecta a la regla especial, se prevé que en las transferencias sujetas al denominado "*puerto seguro*" se acredite "*que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión*".

Ello se debe a la complejidad del régimen de "puerto seguro", constituido por una serie de principios de autorregulación a los que las entidades de los Estados Unidos podrán libremente adherirse. El único modo de comprobar la existencia de dicha adhesión, que impone el sometimiento a la decisión de un Organismo público de los Estados Unidos es que aquél certifique la efectividad de esa adhesión. Por ello, la transferencia será posible siempre que se aporte esa certificación.

[25] Mediante la Decisión de la Comisión Europea 2000/520/CE, de 26 de julio se autorizaba la transferencia de datos de carácter personal entre la UE y los EE.UU.

[26] El 1 de enero de 2002, la Comisión Europea reconoció que Canadá tenía un régimen adecuado de protección con lo que autorizaba la transferencia de datos de carácter personal entre la UE y Canadá.

3) Transferencia a países que no ofrezcan un nivel adecuado de protección.

Como ya se expuso, en este caso es posible la transferencia internacional de datos siempre que la misma o bien se encuentre amparada por una de las excepciones específicas que establece el artículo 34 de la LOPD, o bien haya sido objeto de una expresa autorización del Director de la APD.

E) Especialidades en caso de tratamiento por cuenta del transmitente.

Por último, la Norma sexta recoge las especialidades en caso de que el destinatario se limite a realizar una actividad por cuenta del transmitente de los datos, en términos similares a los establecidos en el artículo 12 de la LOPD.

En este caso, y sin perjuicio del cumplimiento de las previsiones que correspondan, atendiendo al país en que se ubique el destinatario, será necesaria la existencia de un contrato escrito que regule la prestación. Dicho contrato deberá indicar expresamente "*que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normas de protección de datos del Derecho español*", debiendo además restituir o destruir los datos al término del contrato y no cederlos, ni siquiera para su conservación, a terceras personas.

Como especialidades, se prevé que los datos no podrán ser objeto de subcontratación por el destinatario de los mismos y que el contrato deberá hacer constar "*la responsabilidad directa de la transmitente como consecuencia de cualquier incumplimiento de la Ley en que incurriera el destinatario*".

II. TRANSFERENCIAS A ENTIDADES UBICADAS EN LOS EE.UU.[27].

1. Marco normativo del sistema de Principios de Puerto Seguro.

39. La Directiva 95/46/CE, que entró en vigor en 1998, supuso el inicio de una disputa entre la UE y EE.UU., pues a los ojos de la Directiva, era posible que las exportaciones de datos de carácter personal a los EE.UU. fueran prohibidas ya que mientras el enfoque de EEUU en

[27] *Vid.* ARRIBAS LUQUE, J. M., "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: el sistema de principios de puerto seguro", en *La Ley*, núm. 5497, 7 de marzo de 2002.

esta materia se basaba en una mezcla de legislación, reglamentación y autorregulación, la UE consideraba imprescindible la protección del derecho fundamental a la privacidad. Tras largas negociaciones, el pasado 29 de julio de 2000, llegaron a un acuerdo, denominado *"Safe Harbour"* (Puerto Seguro) por el que se establecía el sistema de Principios de Puerto Seguro para la protección de la vida privada. Se trata de un sistema eficaz, tanto desde el punto de vista teórico como desde el punto de vista práctico, ya que posibilita un flujo estable e ininterrumpido de información asegurando un nivel permanente de protección adecuada [28].

40. El sistema de Principios de Puerto Seguro presenta numerosas ventajas, teniendo en cuenta que: a) Constituye un marco normativo uniforme, permanente, estable y definitivo para la protección del derecho a la intimidad y para la transferencia internacional de datos de carácter personal entre la UE y los EE.UU.; b) Permite la aprobación automática por todos los Estados miembros de la UE de las transferencias internacionales de datos de carácter personal con destino a los EE.UU.; y, c) Sustituye a las legislaciones internas de cada uno de los Estados miembros de la UE.

41. El sistema de Principios de Puerto Seguro se configura, entonces, como un programa voluntario, basado en la autocertificación y en la autoevaluación, que se ofrece a las entidades de los EE.UU. con el fin de obtener, respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida a nivel comunitario, que permite asegurar, de manera permanente, la legitimidad de las transferencias internacionales de datos de carácter personal.

El sistema ha estado disponible para las empresas estadounidenses desde el pasado 1 de noviembre de 2000, teniendo una duración, en principio, ilimitada, aunque existen dos revisiones, programadas, una para el 1 de junio de 2001 y otra para el 2003, todavía no efectuadas, y una advertencia de revocación en caso de uso fraudulento.

2. Contenido del sistema de Principios de Puerto Seguro.

42. Llegados a este punto, se hace necesario el estudio de la estructura normativa de los Principios de Puerto Seguro, que combina las siguientes normas: a) Por un lado, unos Principios de Puerto Seguro para la protección de la vida privada, que fueron publicados por el *US Department of Commerce*, el pasado 21 de julio de 1998; b) Por otro lado, por unas

[28] Desde un punto de vista práctico, a 29 de enero de 2002, son ya 148 empresas las que se han adherido al Sistema (Microsoft Corporation; Intel; Doubleclick, Inc.; Hewlett Packard; BMW Group, Inc, etc.) aunque la regla general es el incumplimiento de las disposiciones de la Directiva 95/46/CEE por parte de las empresas estadounidenses.

Frecuentley Asked Questions (FAQ), publicadas también por el *US Department of Commerce*, el pasado 4 de julio de 2000, con el objeto de servir de guía para la aplicación de los Principios antes mencionados; y, finalmente, c) Por la Decisión de la Comisión Europea 2000/520/CE, de 26 de julio, con arreglo a la Directiva 95/46/CEE, del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de los Estados Unidos de América[29].

Los Principios de Puerto Seguro, que tienen fuerza vinculante, desde el punto de vista de su estructura formal, es de destacar que, a) Van precedidos de una introducción, que contiene una advertencia y diversas instrucciones sobre la forma de adhesión al sistema por parte de las entidades estadounidenses y la jurisdicción competente para la interpretación de los referidos Principios; y, b) Van seguidos de un anexo con los organismos de los EE.UU. reconocidos por la UE para la investigación de quejas y la solicitud de medidas provisionales.

Las *Frecuentley Asked Questions (FAQ)* son quince y tiene por objeto, a modo de guía, aclarar y, en algunos casos, culminar, siendo de gran ayuda a las instancias encargadas de interpretar y aplicar los Principios de Puerto Seguro.

La *Decisión de la Comisión Europea 2000/520/CE, de 26 de julio* consta de once considerandos y cinco artículos, donde establece las condiciones que deben cumplirse en cada transferencia de datos de carácter personal para que se entienda que existente la equivalencia, una presunción de cumplimiento de dichas condiciones, las posibilidades de suspensión de transferencias y de modificación de la Decisión, el reconocimiento de competencia de determinados organismos de los EE.UU. para investigar quejas y solicitar medidas provisionales y reparaciones para los particulares, independientemente de su residencia y nacionalidad y, la obligación de los destinatarios (que son los Estados miembros de la UE) de la norma de adoptar las medidas necesarias para su cumplimiento.

43. Los Principios de Puerto Seguro, que se configuran como mínimos para cualquier política privada de protección de datos de carácter personal, son los siguientes:

1) Principio de Notificación ("*Notice*"): establece la obligación que tienen las entidades de informar a los particulares de los fines y utilización de sus datos de carácter personal.

2) Principio de Opción ("*Choice*"): dispone la obligación de las entidades de ofrecer a los particulares la posibilidad de decidir si su datos de carácter personal pueden ser o no cedidos a un tercero.

[29] D.O. L 215, de 25 de agosto de 2000; corr. de errores en D.O. L 115, de 25 de abril de 2001.

3) Principio de Transferencia Ulterior ("*Onward Transfer*"): señala que para revelar información a terceros que no participen en el sistema de Puerto Seguro, las entidades deberán aplicar los Principios de notificación y de opción.

4) Principio de Seguridad ("*Security*"): establece que las entidades que se encargan de la recogida de datos de carácter personal deberán tomar todas las precauciones que estimen oportunas con el fin de evitar su pérdida, modificación o destrucción.

5) Principio de Integridad de los datos ("*Data Integrity*"): señala que los datos de carácter personal deben ser pertinentes con respecto a los fines con los que se utiliza.

6) Principio de Acceso ("*Access*"): recoge el derecho de los particulares al conocimiento de de sus datos de carácter personal que las entidades tengan sobre ellos y poder corregirla, modificarla o suprimirla en caso de que sea inexacta.

7) Principio de Aplicación ("*Enforcement*"): dispone la necesidad de incluir una vía de recurso para los interesados que se vean afectados por el incumplimiento de la normativa sobre transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

44. No obstante, existen toda una serie de excepciones a estos Principios del sistema de Puerto Seguro, a saber: a) Cuando sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) Cuando una disposición legal o resolución jurisdiccional así lo establezca; y, c) Cuando la Directiva 95/46/CEE o cualquier norma de los Estados miembros de la UE lo permita.

3. Incumplimiento de los Principios de Puerto Seguro.

45. En definitiva, en cumplimiento de la Directiva 95/46/CEE, las entidades estadounidenses pueden adoptar cualquiera de las siguientes posturas: a) Adherirse al sistema de Principios de Puerto Seguro; b) Acudir a fórmulas que exoneren del requisito de la protección adecuada, que recoge el artículo 26 de la Directiva 95/46/CEE; y, c) No recibir datos de carácter personal de la UE.

46. Ante el incumplimiento por parte de las entidades estadounidenses del sistema de Puerto Seguro, caben dos posibilidades:

a) La suspensión de las transferencias de datos de carácter personal hacia una entidad que haya autocertificado su adhesión a los Principios y su aplicación de conformidad con las

FAQ, con el fin de proteger a los particulares de un "tratamiento fraudulento" de sus datos de carácter personal, o la adopción de cualquier otra medida dentro de sus competencias con el fin de evitar ese "tratamiento fraudulento" de los datos de carácter personal de los particulares.

En este sentido, hablamos de "tratamiento fraudulento" cuando existan grandes probabilidades de que se estén vulnerando los Principios del Puerto Seguro, existan razones para creer que el mecanismo de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión, la transferencia en cuestión pueda crear un riesgo inminente de grave perjuicio a los afectados o las autoridades competentes del Estado miembro de la UE hayan realizado notables esfuerzos para notificárselo a la entidad y proporcionarle la oportunidad de alegar en su defensa lo que estimen oportunos para evitar la imposición de una medida tendente a suspender la transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

b) Si se demostrara que un organismo encargado del cumplimiento de los Principios de Puerto Seguro en los EE.UU. no está ejerciendo su función, la Comisión Europea le notificará al *US Department of Commerce* que tiene intención de adoptar toda una serie de medidas[30] con el objeto de anular, suspender o restringir la transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

[30] Las medidas a adoptar por parte de la Comisión Europea serán aplicadas con arreglo al procedimiento previsto en el artículo 31 de la Directiva 95/46/CEE

CONCLUSIONES FINALES.

47. A modo de conclusión, podríamos destacar las siguientes ideas:

1º) Las nuevas tecnologías permiten no sólo nuevas, más fáciles y más sofisticadas formas de comunicación, sino también, y como contrapartida, la posibilidad técnica de que se produzcan más injerencias en las mismas. Ahora bien, como ya hemos comprobado, si bien es cierto que *Internet* no es un vacío jurídico en materia de tratamiento informatizado de datos de carácter personal y la protección de la intimidad, no es menos cierto que: a) La protección efectiva de la intimidad en *Internet* necesita de una acción combinada entre poder público[31] y actores privados; b) Es necesaria la combinación de la regulación y la autorregulación por parte de los actores de *Internet*; c) En la medida en que las respuestas nacionales son insuficientes, en ocasiones, se pone de manifiesto la necesidad de cooperación internacional.

2º) El uso de *Internet* implica riesgos para el derecho a la protección de datos de carácter personal, en el sentido de que se generan importantes datos que sin el consentimiento de los afectados pueden ser almacenados por terceros.[32]

3º) Como hemos podido comprobar la normativa española en materia de protección de datos de carácter personal, esto es, fundamentalmente la LOPD, es una de las normativas europeas más restrictivas y complejas en esta materia ya que, prácticamente cualquiera que desarrolle una actividad, sea cual sea, debe cumplir con la normativa vigente. La complejidad y el carácter restrictivo de la LOPD implican, en ocasiones, la imposibilidad de su cumplimiento. La LOPD impone unas obligaciones legales y técnicas que no están al alcance de la mayor parte de las empresas españolas. Nos produce mayor preocupación el hecho de que ni siquiera algo tan evidente y fácil de realizar como es la inscripción de los ficheros en el RGPD de la APD se efectúe, como consecuencia del desconocimiento generalizado que existe acerca de la normativa en materia de protección de datos de carácter personal[33].

---

[31] En este sentido, la Comisión Europea está analizando la posibilidad de publicar unas recomendaciones para la protección de las personas físicas en relación con la recogida y el tratamiento automatizado de datos personales a través de las autopistas de la información.

[32] Así, por ejemplo, en EEUU se interpuso en enero de 2000 una querella contra la empresa Doubleclik ya que se dedicaba a comercializar los datos de sus clientes cuando accedían a su *web*.

[33] Así, según han alertado las Cámaras de Comercio, Industria y Navegación, el 95 % de las PYMES están, en la actualidad, incumpliendo la LOPD. A fecha de septiembre de 2002, tan sólo 167.000 empresas habían registrado sus ficheros en el RGPD.

4º) Es evidente que la LOPD obliga a los responsables de los ficheros a cumplir una serie de obligaciones pero, no es menos importante intentar concienciar a los interesados y/o afectados de que se debe establecer una política de seguridad de forma que se establezcan unos mecanismos y procedimientos mediante los cuales se salvaguarden sus sistemas informáticos y la información que en ellos se contiene. Como ha dejado claro más de una vez la APD, "*debemos evitar que la informática invada nuestra intimidad"*.

5º) Hemos hecho referencia a la LSSI, pues bien, no debemos olvidar que ésta deberá ser modificada en breve como consecuencia de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, ya que si bien el artículo 21 de la LSSI prohíbe el envío de comunicaciones comerciales electrónicas que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas y, el artículo 22 de la LSSI dispone, por un lado, que *"si el destinatario de servicios debiera facilitar su dirección de correo electrónico durante el proceso de contratación o de suscripción a algún servicio y el prestador pretendiera utilizarla posteriormente para el envío de comunicaciones comerciales, deberá poner en conocimiento de su cliente esa intención y solicitar su consentimiento para la recepción de dichas comunicaciones, antes de finalizar el procedimiento de contratación";* y, por otro lado, que *"el destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente";* la Directiva 2002/58/CE establece todo lo contrario al señalar, en su artículo 13, que cuando una persona física o jurídica obtenga de sus clientes su *email*, en el contexto de la venta de un producto o de un servicio, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente, no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior. No olvidemos que España deberá incorporar esta Directiva al régimen normativo interno no más tarde del próximo 31 de octubre de 2003, por lo que nos vamos a poder encontrar hasta la fecha con situaciones tales como que una empresa española sea sancionada por el envío de *emails* publicitarios a sus propios clientes, conducta prohibida por la LSSI, hasta que, como consecuencia de la Directiva 2002/58/CE, no sea modificada pero permitida por esta última.

6º) El régimen a que se someten los movimientos internacionales de datos de carácter personal se establece en los artículos 33 y 34 de la LOPD. En este sentido se establece que *"no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido*

objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas". Ahora bien, no se permiten transferencias de datos *"a países que no proporcionen un nivel de protección equiparable"* al que ofrece la LOPD, salvo que el transmitente cumpla lo previsto en la LOPD y el Director de la LOPD autorice la transmisión *"si se obtienen las garantías adecuadas".*

7º) Por último, debemos señalar que ante los supuestos de transferencia internacional de datos hay que considerar: a) La naturaleza de los datos que se van a transferir; b) La finalidad del tratamiento que se efectuará en el extranjero; c) La duración de dicho tratamiento; d) El país origen de los datos; e) El país de destino final de los mismos; f) La legislación vigente en el país de destino en materia de protección de datos personales; g) El contenido de los dictámenes emitidos por la Comisión de la UE respecto al nivel de protección que otorgan determinados países en materia de protección de datos personales; h) Concretas normas profesionales, si fueran aplicables; y, j) Las medidas de seguridad que estén en vigor en el país de destino de los datos.

8º) El denominado "Safe Harbour" (Puerto Seguro) por el que se establecía el sistema de Principios de Puerto Seguro para la protección de la vida privada, basado en la voluntaria y libre autocertificación y autoevaluación de las entidades de los EE.UU., tiene como finalidad obtener, respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida a nivel comunitario, que permita asegurar, de manera permanente, la legitimidad de las transferencias.

BIBLIOGRAFÍA.

Manuales generales

AMADEO GADEA, Santiago Luis, *Informática y Nuevas Tecnologías*, La Ley-Actualidad, Madrid, 2001.

DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de Derecho Informático*, 4ª edición, Aranzadi, Elcano (Navarra), 2002.

DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet*, Civitas, 3ª edición, Madrid, 2002.

ESTEVE GONZÁLEZ, Lydia (Coord.) y otros, *Derecho e Internet. Textos Jurídicos Básicos*, Editorial Compás, Alicante, 2001.

Monografías

AA.VV., *Introducción a la informática para Juristas*, Editorial Club Universitario (ECU), Alicante, 1997.

AA.VV., *Problemática jurídica en torno al fenómeno de Internet*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2000.

AA. VV., *Protección y seguridad de datos. Nuevo marco legal relativo a la protección y seguridad de datos de carácter personal*, Recoletos, Madrid, 2000.

AA.VV., Guía práctica de la Ley Orgánica de Protección de datos, edición en cd-rom, Deloitte & Touche, 2002.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Navarra, 1999.

ÁLVAREZ CIVANTOS, Oscar José, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Editorial Comares, Granada, 2001.

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

APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, Editorial Comares, Granada, 2002.

BERTRAND, André y PIETTE-COUDOL, Thierry, *Internet et le droit*, Presses Universitaires de France, Paris, 1999.

CALVO CARAVACA, Alfonso Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001.

CAMPUZANO, Herminia, *Vida privada y datos personales,* Madrid, Tecnos, 2000.

CLIMENT BARBERÁ, Juan, *Derecho y nuevas tecnologías*, Servicio de Publicaciones de la Universidad Cardenal Herrera-CEU, Valencia, 2001.

COLLADO GARCíA-LAJARA, E., *Protección de datos de carácter personal. Legislación, Comentarios, Concordancias y Jurisprudencia*, Dykinson, Madrid, 2000.

CORREDOIRA Y ALFONSO, Loreto, *La libertad de información. Gobierno y Arquitectura de Internet*, III Seminario de Telecomunicaciones e Información, Madrid, 2001.

DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de datos en Europa*, Ansef, Madrid, 1998.

DAVARA RODRÍGUEZ, Miguel Ángel, *Nueva guía práctica de protección de datos desde la óptica del titular del fichero*, Dykinson, Madrid, 2001.

DE ROSSELLO MORENO, Rocío, *El Comercio Electrónico y la protección del consumidor*, Cedecs Editorial, Barcelona, 2001.

DEL PESO, E. y RAMOS, M. A., *LORTAD. Reglamento de seguridad*, Díaz de Santos, Madrid, 1999.

DEL PESO NAVARRO, Emilio, *Ley de Protección de Datos. La nueva LORTAD*, Ediciones Díaz de Santos, Madrid, 2000.

ÉCIJA BERNAL, Álvaro y SÁIZ PEÑA, Carlos A. (Coordinadores), *Contratos de Internet. Modelos y Comentarios Prácticos*, Aranzadi, Elcano (Navarra), 2002.

ESTADELLA YUSTE, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995.

FERNÁNDEZ GÓMEZ, Eva, *Comercio electrónico*, McGraw-Hill, Madrid, 2002.

GARRIGA DOMÍNGUEZ, Ana, *La protección de los datos personales en el Derecho español*, Dykinson, Madrid, 1999.

GÓMEZ GAMBOA, D., *El tratamiento automatizado de datos frente a los derechos fundamentales al honor, intimidad y protección de datos de carácter personal*, Dykinson, Madrid, 2001.

GÓMEZ SEGADE, José Antonio (Dir.) y otros, *Comercio electrónico en Internet*, Marcial Pons, Madrid, 2001.

GONZÁLEZ MÉNDEZ, Amelia, *La protección de datos tributarios y su marco constitucional*, Tirant lo blanch, Valencia, 2003.

GRIMALT SERVERA, Pedro, *La responsabilidad civil en el tratamiento automatizado de los datos de carácter personal*, Comares, Granada, 1999.

HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal*, Tecnos, Madrid, 1996.

HERRÁN ORTIZ, Ana Isabel, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson, Madrid, 2002.

HERRÁN ORTIZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999.

LAGARES GARCÍA, Diego, *Internet y El derecho. Tecnología y Jurisprudencia: dos conceptos obligados a entenderse*, Ediciones Carena, Barcelona, 2000.

LLANEZA GONZÁLEZ, Paloma, *Aplicación práctica de la LSSI-CE. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico*, Editorial Bosch, Barcelona, 2003.

MÉNDEZ, Rosa M. y VILALTA, A. Esther, *Obligaciones y responsabilidad de los prestadores de servicios de la sociedad de la información. La acción de cesación (L. 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico)*, Editorial Bosch, Barcelona, 2003.

MONTESINOS GUTIÉRREZ, Antonio, *La sociedad de la información e Internet*, San Pablo, Madrid, 1999.

MORENO NAVARRETE, Miguel Ángel, *Contratos electrónicos*, Marcial Pons, Madrid, 1999.

MUÑOZ MACHADO, Santiago, *La regulación de la red. Poder y Derecho en Internet*, Taurus, Madrid, 2000.

ORTÍ VALLEJO, Antonio y GUTIÉRREZ JEREZ, Luis Javier, *Legislación sobre datos de carácter personal*, Tecnos, 2ª edición, Madrid, 2000.

RUIZ CARRILLO, Antonio, *La protección de los datos de carácter personal*, Editorial Bosch, Barcelona, 2001.

SÁNCHEZ ALMEIDA, Carlos y MAESTRE RODRÍGUEZ, Javier A., *La Ley de Internet. Régimen jurídico de los Servicios de la Sociedad de la Información y Comercio Electrónico*, SERVIDOC, Barcelona, 2002.

TÉLLEZ AGUILERA, A., *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Dykinson, Madrid, 2001.

VELÁZQUEZ BAUTISTA, Rafael, *Derecho de tecnologías de la información y las comunicaciones (T.I.C.)*, 1ª edición, Colex, Madrid, 2001.

VIZCAÍNO CALDERÓN, Miguel, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001.

Estudios en obras colectivas

APARICIO SALOM, Javier, "Nueva Ley de protección de datos de carácter personal. Preguntas y respuestas", en *Nueva Ley de protección de datos de carácter personal y reglamento de medidas de seguridad informática*, Madrid, 2000, pp. 23 y ss.

APARICIO SALOM, Javier y FERNÁNDEZ-SAMANIEGO, Javier, "Reglamento de medidas de seguridad. Preguntas y respuestas", en *Nueva Ley de protección de datos de carácter personal y reglamento de medidas de seguridad informática*, Madrid, 2000, pp. 41 y ss.

BALSANO, Anna Maria, "An International Legal Instrument for Cyberspace? A Comparative Analysis with the Law of Outer Space", en *The International Dimensions of Cyberspace Law*, Ashgate, Burlington USA, 2000, pp. 127-145.

CAVANILLAS MÚGICA, Santiago, "La responsabilidad civil de los servicios de la sociedad de la información en la utilización de las nuevas tecnologías de la comunicación" en *Perfiles de la responsabilidad civil en el nuevo milenio*, Madrid, Dykinson, 2000, pp. 123-128.

CHARLESWORTH, A., "Data Privacy in Cyberspace: Not national vs. International but Commercial vs. Individual", en *Law and the Internet. A Framework for Electronic Commerce*, Oxford, Hart, 2ª edición, 2000, pp. 79-122.

DE ASÍS ROIG, A. E., "Protección de Datos y Derecho de las telecomunicaciones", en *Régimen jurídico de Internet*, La Ley-Actualidad, Madrid, 2002.

FERNÁNDEZ SAMANIEGO, Javier, "La nueva Ley de Protección de Datos de carácter personal española (Ley Orgánica 15/1999, de 13 de diciembre), en *Nueva Ley de protección de datos de carácter personal y reglamento de medidas de seguridad informática*, Madrid, 2000, pp. 17 y ss.

LONGWORTH, Elizabeth, "The Possibilities for a Legal Framework for Cyberspace- including a New Zealand Perspective", en *The International Dimensions of Cyberspace Law*, Ashgate, Burlington USA, 2000, pp. 9-69.

MACKENZIE, John S., "Setting up a Legal Web Site: Pitfalls and Promises", en *Law and the Internet. A Framework for Electronic Commerce*, Oxford, Hart, 2ª edition, 2000, pp. 27-41.

RIBAS ALEJANDRO, Javier, "Riesgos legales en Internet. Especial referencia a la protección de datos personales", en *Derecho de Internet. Contratación electrónica y firma digital*, Aranzadi, Elcano (Navarra), 2000, pp. 143-160.

ROCA JUNYENT, M. Y TORRALBA MENDIOLA, E., "Derecho a la intimidad: el secreto de las comunicaciones e Internet" en *Régimen Jurídico de Internet*, La Ley, Madrid, 2002.

ROSSET, Arthur, "La regulación legislativa del comercio electrónico: una perspectiva americana", en *Derecho del comercio electrónico*, La Ley-Actualidad, S.A., Madrid, 2001, pp. 57-74.

RUIZ MIGUEL, Carlos, "Protección de datos personales y comercio electrónico" en *Comercio electrónico en Internet*, Marcial Pons, Madrid, 2001.

TERRETT, Andrew and MONAGHAN, Iain, "The Internet- An Introduction For Lawyers", en *Law and the Internet. A Framework for Electronic Commerce*, Oxford, Hart, 2ª edition, 2000, pp. 1-13.

TORREMANS, Paul, "Private International Law Aspects of IP- Internet Disputes", en *Law and the Internet. A Framework for Electronic Commerce*, Oxford, Hart, 2ª edición, 2000, pp. 225-246.

Estudios en revistas

ABAD MOROS, Mª Rosa, "El recurso de inconstitucionalidad del Defensor del Pueblo contra la LO 15/99, de Protección de Datos de Carácter Personal", en *REDI: Revista Electrónica de Derecho Informático,* núm. 28, 2000.

ALONSO MARTÍNEZ, Carlos, "Aproximación a determinados conceptos del RD 994/99, de 11 de junio, sobre medidas de seguridad", en *Actualidad Informática Aranzadi,* núm. 35, 2000.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., "Notas a la nueva regulación de la protección de datos de carácter personal", en *La Ley*, núm. 5036, 17 de abril de 2000, pp. 1709-1716.

ARRIBAS LUQUE, J. M., "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: el sistema de principios de puerto seguro", en *La Ley*, núm. 5497, 7 de marzo de 2002.

BURNSTEIN, Matthew, "Conflicts on the Net: Choice of Law in Transnational Cyberspace", en *Vanderbilt Journal of Transnational Law*, vol. 29, January 1996, nº 1, pp. 75-116.

CARRASCOSA GONZÁLEZ, Javier, "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado", en *Revista Española de Derecho Internacional,* vol. XLIV, núm. 2, 1992, pp. 417-441.

CARRASCOSA GONZÁLEZ, Javier, "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE, en *Actualidad Civil*, núm. 23, 1997, pp. 509-539.

CORRIPIO GIL-DELGADO, María De los Reyes, "La protección de datos personales en Internet", en *Boletín Informativo del Ministerio del Interior*, nº 1901, pp. 2913-2927.

DAVARA RODRÍGUEZ, Miguel Ángel, "Los principios de la protección de datos y los derechos de las personas en la nueva Ley Orgánica de Protección de Datos de Carácter Personal", en *Actualidad Informática Aranzadi*, Editorial Aranzadi, Elcano (Navarra), 2000.

FERNÁNDEZ LÓPEZ, Juan Manuel, "La nueva Ley de protección de Datos de Carácter Personal. Su por qué y sus principales novedades", en *Actualidad Informática Aranzadi*, 2000.

GARCÍA MESEGUER, María Dolores y MEDRÁN VIOQUE, Rafael, "La protección de datos de las personas en el tratamiento de datos: Principios y Derechos. Breve comentario de la

transposición de la Directiva 95/46/CE a la Ley Orgánica 15/99", en *Revista electrónica V-lex*, 2002.

GARCÍA ONTOSO, Rosa María, "Comentarios a la nueva Ley de Datos de Carácter Personal de 13 de diciembre", en *Actualidad Informática Aranzadi*, Editorial Aranzadi, Elcano (Navarra), 2000.

GAUTRAIS, Vicent, LEFEBVRE, Guy et BENYEKHLEF, Karim, "Droit du Commerce électronique et normes applicables: l´emergence de la *lex electronica*", en *Revue de Droit des Affaires Internationales*, nº 5, 1997, pp. 547-583.

MAESTRE, Javier A., "Comentarios a la nueva legislación sobre protección de datos", en *REDI: Revista Electrónica de Derecho Informático*, Número 21, abril 2000.

MANRESA FARRERAS, B., "Los datos personales en la legislación en materia de protección de datos: ¿Qué debe entenderse por dato de carácter personal?, en *REDI: Revista Electrónica de Derecho Informático*, núm. 45, 16 de marzo de 2002.

MARTÍNEZ-CASALLO LÓPEZ, Juan José, "Implicaciones de la Directiva sobre protección de datos en la normativa española", en *Actualidad Informática Aranzadi,* núm. 20, julio de 1996.

MARTÍNEZ SÁNCHEZ, Mar, "Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal", en *Actualidad Informática Aranzadi,* núm. 35, abril de 2000.

MARZO, Ana., "Novedades de la Ley de Protección de Datos", en *Revista IURIS*, Madrid, 2002, pp. 42-47.

MAYOL GIL, Juan Antonio, MEDRÁN VIOQUE, Rafael y ORTEGA GIMÉNEZ, Alfonso, "Data Protection in Internet", en *REDI: Revista Electrónica de Derecho Informático*, núm. 50, 2002.

MAYOL GIL, Juan Antonio, MEDRÁN VIOQUE, Rafael, MIESKES, Manfred y ORTEGA GIMÉNEZ, Alfonso, "Comparative analysis between spanish and german law concerning data protection in internet" en *uaipit.com -Portal de la Universidad de Alicante sobre Propiedad*

Industrial e Intelectual y Sociedad de la Información- (http://www.uaipit.com/en/ITL/Data_Protection_Internet.pdf), 2003.

MORENO DE LA SANTA GARCÍA, Enrique, "Retos para el jurista en Internet" en *IURIS. Actualidad y Práctica del Derecho*, La Ley, Madrid, Enero 2001

ORTEGA GIMÉNEZ, Alfonso, "Censo promocional y consentimiento del afectado" en *IURIS. Actualidad y Práctica del Derecho, Número 68*, La Ley, Madrid, Enero 2003.

PÉREZ DE VELASCO, José Ramón, "Protección de Datos de Carácter personal", en *REDI: Revista Electrónica de Derecho Informático*, núm. 27, octubre de 2000.

ROCA JUNYENT, M. Y TORRALBA MENDIOLA, E., "Ley de Protección de datos", en *La Ley*, núm. 5014, 16 de marzo de 2000, pp. 1733-1736.

VIGURI PEREA, Agustín, "Intimidad versus informática. La protección de datos personales: perspectiva desde el Derecho comparado", en *La Ley*, núm. 2, 1999.