

**RECOMENDACIONES DE LA AGENCIA DE PROTECCIÓN DE DATOS AL SECTOR DEL COMERCIO ELECTRÓNICO, PARA LA ADECUACIÓN DE SU FUNCIONAMIENTO A LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

Durante los meses de septiembre, octubre y noviembre de 2000, la Agencia de protección de Datos llevó a cabo una inspección sectorial cuyo objetivo era determinar si las entidades que actualmente desarrollan su actividad comercial a través de Internet cumplen con los principios de la legislación vigente en materia de protección de datos, así como coadyuvar al cumplimiento de la misma, a cuyo efecto el Plan de Inspección culmina con las pertinentes Recomendaciones, en las que se recogen los criterios que han de seguir las entidades inspeccionadas para el mejor cumplimiento de la ley.

En el transcurso de esta inspección se analizaron dos de las modalidades de comercio electrónico en las que el ciudadano tiene una clara participación: la que se establece entre empresa y consumidor (B2C) y la venta directa entre consumidores (C2C). Por otra parte, el análisis se circunscribió a las entidades que comercian a través de la Red, dejando de momento a un lado a aquellas otras que tan sólo disponen de portales generalistas entre cuyos servicios no se ofrece la adquisición on-line de productos o servicios, a pesar de que también estas compañías recaban gran cantidad de datos sobre los usuarios que deciden registrarse. En este sentido, sólo se incluyeron

en nuestro análisis algunos portales que sí realizaban actividades de comercio electrónico. Las conclusiones vertidas aquí, por tanto, se han obtenido como resultado de las actuaciones de inspección practicadas en las denominadas "*tiendas virtuales*", entendiendo como tales las webs que permiten al usuario la compra, directa o indirectamente, de un producto o servicio, de forma tal que la transacción comercial (a excepción de la entrega del bien adquirido) quede cerrada on-line.

Se analizaron 44 webs desde las que se desarrollaban actividades de comercio electrónico. Considerando la gran diversidad existente en el sector, en la inspección se optó por seleccionar varios representantes de cada uno de los siguientes grupos:

- Portales generalistas: webs que, aparte de ofrecer servicios electrónicos como noticias, correo web o foros, incorporan además la venta de productos o servicios en general.
- Grandes centros comerciales: versión electrónica de algunos grandes centros comerciales ("*híper*", "*súper*").
- Tiendas especializadas en la venta de determinados productos y servicios: libros, música, cine, bebidas alcohólicas, viajes, ocio, cosmética, informática o telecomunicaciones.
- Intermediarios comerciales: webs que no son tiendas propiamente dichas pero desde las cuales el usuario puede seleccionar la tienda virtual que más se adecua a sus necesidades ("*buscadores de tiendas*") y también aquéllas otras webs desde las que los usuarios compran y venden sus propios productos siguiendo la modalidad de subasta.

En la totalidad de las webs analizadas se pudo determinar el nombre de la compañía que había registrado el dominio correspondiente en Internet, verificándose por el contrario que no siempre se informaba desde la propia web del nombre del responsable del fichero en el que se incorporan los datos personales recabados. En este sentido, se comprobó también que en 12 de las 44 webs analizadas (27%) no se hacía ninguna referencia a la información que establece el apartado 1 del artículo 5 de la LOPD, mientras que en el resto sí se incluía un texto con el que se pretende cubrir en mejor o peor medida ese requisito legal.

También se verificó que, a la fecha de la inspección, los responsables de 16 de las 44 webs analizadas (36%) no figuraban aún inscritos en el Registro General de Protección de Datos, cuando en la práctica totalidad de los casos resultaba evidente que recababan datos personales desde las citadas webs. Se comprobó que, en la mayor parte de los casos, los usuarios deben registrarse con carácter previo a la realización del oportuno pedido, facilitando para ello sus datos identificativos (nombre completo, dirección postal, dirección electrónica, número de teléfono) y, en ocasiones, edad o fecha de nacimiento, número de D.N.I. Una vez registrado, el usuario dispone de un código que le permitirá identificarse (generalmente coincidente con su dirección electrónica) y una contraseña para autenticar su identidad.

**DE ESTA FORMA, AL REALIZAR CADA PEDIDO SÓLO TENDRÁ QUE IDENTIFICARSE, SIN NECESIDAD DE FACILITAR EN CADA OCASIÓN SUS DATOS**

PERSONALES. GENERALMENTE, TODAS LAS COMPRAS REALIZADAS A TRAVÉS DE LA WEB QUEDARÁN ASOCIADAS AL IDENTIFICADOR DE USUARIO SELECCIONADO. POR OTRA PARTE, SI EL USUARIO DECIDE REALIZAR EL PAGO MEDIANTE SU TARJETA DE CRÉDITO/DÉBITO, CADA VEZ QUE REALIZA UNA COMPRA DEBE TAMBIÉN FACILITAR EL CÓDIGO IDENTIFICATIVO DE LA MISMA (16 DÍGITOS) Y SU FECHA DE CADUCIDAD.

En materia de seguridad, de las 44 webs analizadas sólo 24 (54%) utilizaban el protocolo *HTTPS (SSL)* para establecer un “canal seguro” de comunicación entre el servidor y el usuario para el envío de sus datos personales. Así, los datos se envían cifrados al servidor, de tal forma que, aun en el supuesto de que la línea fuese “escuchada” por terceros no autorizados, éstos no podrían acceder a los datos de forma inteligible. En general, el canal seguro sólo se establece para la recogida de los datos asociados al pedido realizado, entre los que puede figurar, como ya se ha comentado, el código identificativo de la tarjeta de pago. Sin embargo, algunas webs también establecen un canal seguro para la recogida de los datos facilitados por el usuario en el momento de registrarse.

## **1. CONCLUSIONES DE LA INSPECCIÓN**

A continuación, se recopilan algunas de las situaciones más frecuentes o significativas que se han presentado a lo largo de las actuaciones practicadas por la Inspección.

### **1.1 Responsabilidad del tratamiento de datos de carácter personal**

Se ha podido comprobar que en algunas de las tiendas investigadas no se identifica explícitamente al responsable del fichero o tratamiento, lo que deja de alguna forma indefenso al afectado de cara al ejercicio de sus derechos, puesto que, dicha figura jurídica no siempre coincide con la de la entidad o persona que ha registrado el dominio en Internet. Es más, en algunos casos ni siquiera se identifica a ésta última a través de la web, lo que obligaría al afectado a averiguarlo por su cuenta, a través del organismo registrador correspondiente.

Por otra parte, en Internet resulta sencillo navegar entre páginas, de tal forma que con sólo hacer “click” en un icono es posible dejar de visualizar una página ubicada en territorio español para pasar a ver otra página almacenada, por ejemplo, en Estados Unidos. Esta circunstancia hace que, en ocasiones, el usuario crea estar facilitando sus datos personales a una entidad cuando en realidad es otra (radicada probablemente en otro lugar del mundo) la que los está obteniendo, siendo muchos los casos en los que ésta última no se identifica claramente en la web.

### **1.2 Información facilitada en la recogida de datos**

Una de las carencias más notables que se han observado es precisamente la insuficiente información que se facilita al visitante de la tienda en el momento de recabar sus datos personales (cuando el usuario se registra como cliente o cuando efectúa un pedido). Es significativo que en más de la cuarta parte de los casos analizados no se facilite en absoluto la información que prevé la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), en su artículo 5, ni se pueda deducir claramente ésta de la naturaleza de los datos personales recabados ni de las circunstancias en que se recaban.

Por otra parte, las fórmulas informativas utilizadas en el resto de los casos tampoco se ajustan siempre a lo que establece la Ley. Como ya se ha mencionado antes, son numerosas las

webs en las que no se identifica explícitamente al responsable del fichero o del tratamiento, lo que se agrava especialmente en aquellos casos en los que el usuario accede a una página a través de un hipervínculo.

Además, por las especiales características del mundo Internet, en ocasiones resulta complicado para el usuario distinguir claramente la figura del comerciante (con quien realmente el comprador establece la transacción comercial) de la figura de mero intermediario (que pone en contacto -virtual- a ambos). En este sentido, el usuario debería ser consciente de que, una vez que ha facilitado sus datos, éstos pueden pasar por las manos de los distintos intervinientes en el proceso: el que gestiona los servidores web por cuenta del comerciante, el propio comerciante, el que autoriza la transacción financiera, el que se encarga de emitir los documentos que otorgan la titularidad del producto (por ejemplo, una agencia de viajes), el que se encarga de servir el producto (logística), el que se encarga de prestar la atención al cliente... Dado que no siempre coinciden estas figuras en una misma entidad jurídica, es muy importante que el comprador sepa quién de todos ellos es el que finalmente decidirá sobre el uso y finalidad de sus datos personales.

En relación con el ejercicio de los derechos que asisten al ciudadano, por regla general se facilita un buzón electrónico, a través del cual se reciben las solicitudes, aunque no son pocas las compañías que también hacen constar su dirección postal como medio alternativo.

Finalmente, junto con la información preceptiva, algunas compañías han incorporado un aviso acerca de la colocación de "cookies" en el ordenador del usuario, así como de su finalidad, tal y como prevé el artículo 4 del *Código Ético de Protección de Datos Personales en Internet*, de la AECE. De esta forma se logra cumplir en mayor medida con el espíritu de la Ley, dado que la información recabada por este procedimiento no es facilitada voluntariamente por el ciudadano, ni se requiere la intervención de éste.

Generalmente, las webs analizadas incorporan la información a la que se refiere el artículo 5 de la LOPD como cláusulas adicionales a las condiciones generales que rigen la vinculación del vendedor con el comprador, aunque se ha observado que en algunos casos esa información se limita a una mera mención al hecho de que "los datos que nos facilite serán protegidos de acuerdo a la Ley", de lo que no puede deducirse en ningún caso que los derechos del comprador estén convenientemente garantizados.

### 1.3 Datos especialmente protegidos

A través de ninguna de las webs analizadas se recaban del ciudadano datos de los que protege el artículo 7 de la LOPD (ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, comisión de infracciones penales o administrativas). Sin embargo, es evidente que aunque el ciudadano no declare estas circunstancias acerca de sí mismo, sí es posible presumir (aunque sea erróneamente) algunas de ellas en función de su comportamiento como comprador. La gama de especialidades es amplia, pues algunas de estas webs están organizadas de acuerdo a las preferencias del visitante.

En el caso de las sex-shops, por ejemplo, los productos eróticos aparecen en ocasiones clasificados de forma que podrían realizarse categorizaciones de los clientes a partir de su historial de compras, que consta en los ficheros de estas compañías. En estos casos el vendedor no recaba del comprador información acerca de sus preferencias sexuales, sino que se limita a dejar constancia en sus ficheros de los productos que el comprador ha solicitado, los cuales pueden ser

orientativos de unos determinados gustos u orientaciones sexuales, aunque éstos no tengan por qué corresponder necesariamente al comprador.

Resulta especialmente preocupante que sean precisamente las sex-shops las entidades que menos información facilitan al usuario acerca del tratamiento de datos relativos a su persona: ninguna de las cuatro webs analizadas informa de lo especificado en el artículo 5 de la LOPD, ni tampoco se deduce que el usuario haya consentido expresamente en su tratamiento. Lo mismo puede decirse de una web analizada que comercializa productos ortopédicos.

## 1.4 Acceso a los datos por cuenta de terceros

Son muchos los agentes que intervienen en el negocio electrónico. Las compañías vendedoras generalmente restringen su actividad a las tareas puramente comerciales, encargando a otras compañías más especializadas tareas como la atención telefónica, las operaciones logísticas o los servicios informáticos. En los tres supuestos se produce el acceso a los datos personales de los clientes de la compañía por parte de las compañías contratadas, por lo que en los tres casos podría ser de aplicación lo establecido en el artículo 12 de la LOPD.

Como consecuencia de las inspecciones realizadas, se ha podido comprobar que no siempre se atiende adecuadamente a este requisito legal. Sin embargo, son numerosos los documentos contractuales analizados en los que se incluye una estipulación especial relativa a la confidencialidad de los datos, con la que de alguna manera se pretende cubrir esa exigencia legal.

También se han encontrado varios casos en los que los servicios informáticos se prestan por compañías extranjeras establecidas en otros países del mundo. En muchas ocasiones las condiciones aplicables a la prestación del servicio se recogen en un documento-tipo, que utiliza habitualmente el prestador y cuya redacción no se ha adaptado a la legislación española.

Otro de los intervinientes en la transacción comercial a través de Internet es la entidad financiera que actúa como *"pasarela de pago"*. La participación de estas entidades es frecuente, fundamentalmente en webs que son propiedad de grandes compañías y que ofrecen a sus clientes el pago on-line de los productos o servicios solicitados. Para ello, en el momento de efectuar la compra se requieren los datos identificativos de la tarjeta de crédito/débito (número y fecha de caducidad, sin identificar al comprador), datos éstos que en la mayor parte de los casos son remitidos directamente a los servidores de la entidad financiera, quien se encarga de aceptar o

rechazar la transacción tras consultar telemáticamente al correspondiente centro autorizador. Sin embargo, algunas de las compañías inspeccionadas conservan en sus ficheros tales datos con objeto de poder acreditar en el futuro la transacción realizada.

Por otra parte, también se ha podido comprobar que una de las webs analizadas colabora con cierta entidad financiera, la cual a través de la página desde la que se remiten los datos identificativos de la tarjeta, recaba también (aunque de forma opcional) el nombre y la dirección electrónica del comprador, sin que se informe a éste de lo que establece el artículo 5 de la LOPD.

## 1.5 Comunicación de datos

Muchas de las compañías inspeccionadas han manifestado su pertenencia a grandes grupos empresariales cuya actividad se ha diversificado en muy diferentes ámbitos. Como es habitual en otros sectores, las compañías que desarrollan su actividad a través de Internet también han considerado los beneficios de compartir su cartera de clientes con las demás empresas de su grupo, por lo que en su propia web incluyen cláusulas informativas con las que pretenden cubrir el requisito legal del previo consentimiento del interesado. Las fórmulas utilizadas suelen consistir en una referencia a la *"posible cesión de datos a otras empresas del grupo"*, en orden a que tales datos sean utilizados con la finalidad de remitir *"informaciones comerciales de su interés"*. Sin

embargo, es precisamente la diversidad de actividades que pueden coincidir en un mismo grupo lo que puede introducir un elemento de inseguridad de cara al ciudadano, especialmente en casos en los que el grupo está formado por un gran número de compañías. Es evidente, además, que en esos casos el grupo empresarial puede llegar a manejar una información muy completa acerca de los hábitos de las personas con las que las compañías participadas han establecido una relación comercial, circunstancia esta de la que quizá no sean del todo conscientes los clientes.

Por estos motivos, resulta especialmente importante que el ciudadano quede informado por completo acerca de los usos concretos que se realizarán de sus datos personales. En caso contrario, podría producirse una vulneración del principio de finalidad en el tratamiento de los datos.

## 1.6 Movimiento internacional de datos

Al hilo de lo expuesto en el apartado anterior, son también especialmente significativos los casos de compañías multinacionales que disponen de establecimientos comerciales en diversos países del mundo, incluido España. Generalmente se trata de webs cuyo diseño se ha adaptado a

las singularidades nacionales y cuya infraestructura común ha favorecido una gestión centralizada, con el consiguiente ahorro de recursos, tanto humanos como materiales. Este modelo de organización tiene, sin embargo, una repercusión clara en lo relativo a la protección de los datos de los clientes, en función precisamente de las garantías que cada país ofrece. Particularizando en el caso español,

se da la circunstancia de que, por ejemplo, así como datos de clientes extranjeros son accesibles desde la filial española, de la misma manera datos de clientes españoles son accesibles desde los establecimientos de las filiales extranjeras, sin que quepa suponer que aquellos países estén ofreciendo a los ciudadanos las mismas garantías que ofrece la legislación española.

Por otra parte, algunas compañías han optado por encargar los servicios informáticos a otras entidades especializadas que en ocasiones se han establecido en países que no son miembros de la Unión Europea o respecto de los cuales la Comisión de las Comunidades Europeas, no haya declarado que garantizan un nivel de protección adecuado.

Es significativo que uno de los países más frecuentemente elegidos sea precisamente Estados Unidos de América. En este caso, la Comisión Europea ha adoptado una Decisión publicada en el Diario Oficial de 25 de agosto de 2000, considerando la existencia de un nivel de protección adecuado cuando las empresas destinatarias de los datos se adhieran a los principios del puerto seguro y a las correspondientes preguntas más frecuentes publicadas por el Departamento de

Comercio norteamericano. En caso contrario o si no concurre ninguna de las excepciones previstas en el artículo 34 de la LOPD, la compañía está obligada a solicitar la correspondiente autorización del Director de la Agencia, conforme a lo dispuesto en el artículo 33 de la LOPD.

Para solventar esta obligación, algunas de las compañías afectadas han optado por acogerse a la excepción prevista en el apartado e) del citado artículo 34 de la LOPD: que *"el afectado haya dado su consentimiento inequívoco a la transferencia prevista"*.

Así, han incluido entre las cláusulas informativas (que el interesado debe conocer al iniciar su relación comercial con la tienda virtual) un texto, de cuya lectura se desprende que los datos facilitados por el comprador serán almacenados en un fichero ubicado en el país en cuestión. Otras compañías, por el contrario, no han incluido un texto semejante.

## **1.7 Ejercicio de los derechos de acceso, rectificación, oposición y cancelación**

La mayor parte de las compañías han establecido distintas vías para facilitar al ciudadano el ejercicio de los derechos que la Ley le reconoce. Dado que la propia naturaleza de Internet permite una interrelación fácil y rápida entre comprador y vendedor, generalmente se ha utilizado la vía del correo electrónico como fundamental tanto para canalizar las solicitudes de acceso, rectificación, oposición y cancelación, como para remitir las consiguientes contestaciones por parte del responsable del fichero. Así mismo, muchas de las compañías han habilitado una zona especial en la web que permite al usuario consultar fácilmente los datos que constan en su fichero (incluido

el seguimiento de los pedidos realizados), para lo que se requiere que previamente el usuario se identifique y que se autentique su identidad a través de la contraseña que eligió en el momento de registrarse. Esta vía facilita considerablemente al usuario el ejercicio de su derecho de acceso e introduce un mayor nivel de transparencia por parte del responsable del fichero. Aparte de Internet, se ha podido verificar que habitualmente las compañías también ofrecen las vías más clásicas de interrelación entre vendedor y comprador, es decir, la comunicación telefónica (por lo general, un servicio de atención específico) y la comunicación postal (en muchas ocasiones, un apartado de correos).

## **1.8 Seguridad de los datos**

Tras la entrada en vigor del *Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*, aprobado mediante Real Decreto 994/1999, de 11 de junio, todavía hoy siguen existiendo entidades que aún no han elaborado e implantado su propia 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.

En general, puede decirse que los ficheros analizados presentan una estructura de datos tal que, en aplicación del artículo 4 del Reglamento, cabría exigir la adopción de las medidas de seguridad calificadas como de nivel básico, dado que los datos son puramente identificativos o estrictamente relativos a la relación comercial entre vendedor y comprador. No obstante, es preciso considerar dos excepciones. La primera, se refiere a los ficheros, que contienen datos relativos al historial de compra de determinados productos, de cuyo conocimiento podrían desprenderse valoraciones acerca de la salud o la vida sexual de los compradores. En segundo lugar, figuran los ficheros que

contienen un conjunto de datos suficientes que permiten obtener una evaluación de la personalidad del individuo.

En otro orden de cosas, ya se ha mencionado que sólo la mitad de las webs analizadas establecen un "canal seguro" para salvaguardar la confidencialidad en el envío de datos personales, fundamentalmente cuando entre ellos figura la identificación de la tarjeta de pago. Sin embargo, ni siquiera las webs que cifran la información están a salvo de accesos no autorizados a los datos, dado que se ha detectado que en algunos casos se utilizan vías no seguras para la confirmación al usuario de sus propios datos de registro (incluida su contraseña de acceso) o de los datos asociados a su pedido. Son los casos en los que esta información se remite por correo electrónico, no aplicándose en ningún caso procedimientos adicionales de cifrado, de forma tal que esos mensajes

podrían ser captados y leídos por personas suficientemente expertas. También se ha detectado que algunas compañías utilizan las "cookies" como método de autenticación de usuarios, permitiendo a éstos ciertas funcionalidades de la web (entre ellas el acceso a sus datos) por el solo hecho de haberse registrado previamente en la web. De esta forma, en el ordenador del usuario se guarda constancia del identificador que se le asigna en el momento del registro, siendo este nombre

reconocido por el servidor al conectarse nuevamente el usuario a la web, sin requerírsele su contraseña como medio para autenticar su identidad. El resultado es especialmente trascendental en aquellos casos en los que el ordenador desde el que se accede es utilizado por varias personas (por ejemplo, en cibercafés), dado que se permitiría a un usuario acceder a los datos personales de otro usuario previamente registrado en la misma web.

Respecto de las medidas concretas previstas en el Reglamento, una de las que, hasta el momento, han demostrado menor implantación es la que emana de su artículo 10, relativa a la necesidad de que exista un registro para el soporte del procedimiento de notificación y gestión de incidencias. Se ha podido comprobar que este registro existe muy pocas veces y en algunos de estos casos ni siquiera se utiliza de forma habitual.

Otra carencia significativa es la que se ha observado con respecto al requisito legal de que en el contrato de prestación de servicios se estipulen las medidas de seguridad que el encargado del tratamiento está obligado a implementar. Son muy pocas las compañías que incluyen estas estipulaciones.

### **1.9 Notificación e inscripción registral de los ficheros**

Como se ha mencionado antes, en bastantes ocasiones las webs analizadas (desde las que se recaban datos personales, en su práctica totalidad) no se cumple con lo establecido en el artículo 26 de la LOPD. Por otra parte, en muchos casos se ha detectado que en la inscripción del fichero no se ha hecho constar una ubicación que se corresponda con la realidad, especialmente cuando las labores de tratamiento habían sido encargadas a otra compañía, cuya identificación y localización ni siquiera figuran en la inscripción, lo que es aún más significativo en los casos en los que esta última compañía se ha establecido en algún país extranjero.

## **2. RECOMENDACIONES AL SECTOR DEL COMERCIO ELECTRÓNICO**

En el momento de dictar las presentes Recomendaciones se ha producido una coincidencia temporal con el análisis que el Grupo de Trabajo sobre la protección de datos personales integrado por las autoridades competentes de los Estados Miembros de la Unión europea competente -Grupo del art. 29 de la Directiva 45/96/CE- ha realizado respecto de los "requisitos mínimos para la recogida en línea de datos personales". Por ello, en la medida en que los hechos constatados en la inspección permiten aplicar los requisitos del documento citado, las Recomendaciones se adecuan a aquéllos. De este modo, la Agencia Española de Protección de Datos trata de contribuir a la aplicación eficaz y homogénea de las disposiciones nacionales adoptadas en la transposición de las Directivas comunitarias y, aportando el valor añadido de aquel documento, tratar de conseguir detallar, a escala europea, un conjunto mínimo de obligaciones que puedan seguir fácilmente los responsables del tratamiento. En conclusión y teniendo como referencia el resultado de las actuaciones de Inspección llevadas a cabo, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga el art. 5, c) y d) del *Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia*, dicta las siguientes

recomendaciones, que deberán ser observadas por las compañías que realizan transacciones comerciales a través de Internet, al objeto de adecuar éstas a los principios de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD)*, y a la normativa que la desarrolla.

### **PRIMERA: INFORMACIÓN EN LA RECOGIDA DE DATOS**

1. De conformidad con lo establecido por el artículo 5 de la LOPD, los interesados a los que se soliciten datos personales a través de Internet deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de

ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

2. En todas y cada una de las páginas web desde las que se recaben datos de carácter personal se incluirá claramente visible la información a la que hace referencia el artículo 5 de la LOPD, que el usuario deberá poder obtener con facilidad y de forma directa y permanente.

Podrá optarse por incorporar en todas esas páginas un texto o un botón adecuadamente etiquetado que, al ser seleccionado mediante un "click", permita obtener la citada información. No obstante, se considera más adecuada una opción según la cual la lectura de dicha información se presente como ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos a la entidad que los está recabando.

En particular, se especificará claramente el nombre o denominación social y el domicilio del responsable del fichero al que se incorporarán los datos personales solicitados, así como una referencia al código de inscripción asignado por el Registro General de Protección de Datos. Deberá

indicarse también la dirección ante la cual pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición, en el caso de que sea distinta del domicilio especificado, así como el procedimiento que deberán seguir los usuarios, ya sea electrónico, postal, telefónico o cualquier otro que se considere válido.

En el caso de que los datos personales vayan a ser inicialmente incorporados a los ficheros de distintos responsables, se referirá toda la información anterior a cada uno de ellos.

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

En todo caso, la información deberá proporcionarse en el mismo idioma en que se recaban los datos personales.

3. Cuando para realizar una transacción comercial a través de Internet se estén utilizando los servicios de “*pasarela de pago*” prestados por determinadas entidades financieras no se almacenarán datos que puedan relacionar la identificación del medio de pago con la identidad de su titular, salvo que sea preciso para los fines legítimos que se persigan.

4. El usuario deberá estar convenientemente informado en todo caso del momento en que desde una web se transfiere el control a otra web, de tal forma que no pueda albergar dudas al respecto. En este sentido, se considera una buena práctica que el responsable de la web se cerciore de que las webs a las que se transfiere el control cumplen también los términos expresados en la presente Recomendación.

#### **SEGUNDA: CONSENTIMIENTO DEL AFECTADO**

1. De acuerdo con lo que dispone el apartado 1 del artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa o sean de aplicación las excepciones previstas en el apartado 2 del mismo artículo.

2. Cuando un usuario facilita voluntariamente sus datos de carácter personal a través de Internet para una finalidad distinta de la mera ejecución de la transacción comercial, se entenderá que consiente en el tratamiento de los mismos en los términos de los que ha sido convenientemente informado en el momento de la recogida.

3. Siempre que la Ley no lo impida y el afectado haya revocado su consentimiento para el tratamiento de sus datos de carácter personal, el responsable del fichero habilitará los medios oportunos para excluir del tratamiento dichos datos.

#### **TERCERA: USOS Y FINALIDADES**

1. Tal y como dispone el apartado 1 del artículo 4 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.

No se recabarán a través de Internet datos personales cuyo conocimiento por parte del responsable no esté justificado por la finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado. A este respecto, se considera una buena práctica que se facilite

y permita la consulta anónima de sitios comerciales sin solicitar a los usuarios que se identifiquen mediante su nombre, apellidos, dirección electrónica u otros datos.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que ha justificado su recogida. En este sentido, para que tales datos puedan ser usados con una finalidad no compatible con ésta, es imprescindible obtener previamente el consentimiento inequívoco del afectado. Para recabar este consentimiento en Internet, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar su voluntad en uno u otro sentido.

Para que la ausencia de manifestación de la voluntad del usuario pueda producir alguna consecuencia respecto del tratamiento de sus datos, deberá habersele advertido expresamente de esta circunstancia, así como de los efectos de la misma.

3. Cuando se haya previsto que los datos sean utilizados de forma tal que los usuarios de una web puedan ser segmentados o categorizados con fines comerciales, a partir de la información personal y comercial que consta en los ficheros, se informará claramente de esta circunstancia al usuario en el momento de recabar sus datos. Así mismo, se le concederá la facultad de oponerse a esta modalidad de tratamiento, indicándole el procedimiento que deberá seguir en el caso de que decida hacer uso de ella.

4. Si, aparte de los datos personales que facilita voluntariamente el interesado a través de Internet, se utilizan procedimientos automáticos invisibles de recogida de datos relativos a una persona identificada o identificable (*cookies*, datos de navegación, información proporcionada por los navegadores, contenidos activos,...) se informará claramente de esta circunstancia al usuario, *antes* de comenzar la recogida de datos a través de ellos o de desencadenar la conexión del ordenador del usuario con otro sitio web.

Así mismo, se deberá informar al afectado del nombre de dominio del servidor que transmite o activa los procedimientos automáticos de recogida, de la finalidad de los mismos, de su plazo de validez, de si es necesaria o no la aceptación de dichos procedimientos para visitar el sitio web y de la opción de que dispone todo usuario de oponerse a esta modalidad de tratamiento, además de las consecuencias de desactivar la ejecución de dichos procedimientos, cuando dicha opción esté

disponible para el usuario.

5. Cuando los datos recabados a través de Internet vayan a ser utilizados para el envío (postal o electrónico) de información comercial, se informará también de esta circunstancia al usuario en el momento de recabar sus datos. Así mismo, se le concederá la facultad de oponerse a esta modalidad de tratamiento, indicándole el procedimiento que deberá seguir en el caso de que decida hacer uso de ella.

#### **CUARTA: CANCELACIÓN DE DATOS**

1. Según prevé el apartado 5 del artículo 4 de la LOPD, los datos de carácter personal serán cancelados a propia iniciativa del responsable del fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. Igualmente serán cancelados cuando así lo solicite el interesado.

2. No obstante, la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles

responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

3. 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 la persona o entidad responsable del tratamiento y el interesado.

#### **UINTA: DATOS DE SALUD Y DE VIDA SEXUAL**

1. De conformidad con lo establecido en el apartado 3 del artículo 7 de la LOPD, los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

2. Los ficheros con datos acerca de transacciones de adquisición de determinados productos o servicios (por ejemplo, productos eróticos u ortopédicos) podrían contener en ocasiones un conjunto de datos de carácter personal suficientes que permitan ser tratados para obtener una evaluación de la personalidad del individuo, relativa a su salud o a su vida sexual. En tales casos este tratamiento sólo podrá realizarse cuando el afectado haya consentido expresamente.

A estos efectos, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar expresamente su voluntad de que tales datos sean recabados y tratados.

#### **SEXTA: ACCESO A LOS DATOS POR CUENTA DE TERCEROS**

1. De conformidad con lo dispuesto en el apartado 1 del artículo 12 de la LOPD, la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que

figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

2. En el citado contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En particular, estas obligaciones se extenderán a todas aquellas entidades que, como encargados del tratamiento, intervengan en el desarrollo de la relación establecida con los usuarios de la web. A este respecto, el prestador del servicio no podrá utilizar los datos para fin distinto del que conste en el contrato, ni subcontratar la gestión del servicio con terceros, salvo que lo haga en nombre y por cuenta del responsable.

#### **SÉPTIMA: COMUNICACIÓN DE DATOS**

1. Según dispone el apartado 1 del artículo 11 de la LOPD, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. A este respecto se tendrán en cuenta, sin embargo, las excepciones previstas en el

apartado 2 del citado artículo, y en particular, la referida a la situación en la que el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este último caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

2. De acuerdo a lo que establece el apartado 3 del mismo artículo y en consonancia con lo expresado por el apartado 2 de la Recomendación Primera, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

En este sentido, cuando los datos personales recabados a través de Internet vayan a ser comunicados a otras compañías (incluso cuando éstas pertenezcan al mismo grupo empresarial) deberá informarse al usuario, de tal forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos. La información podrá referirse genéricamente a un sector de actividad económica (por ejemplo, servicios financieros,...), sin que puedan admitirse

finalidades indeterminadas o no comprensibles para el usuario (por ejemplo, actividad comercial, actividad publicitaria, empresas del grupo,...).

3. Cuando una compañía transfiere a otra la titularidad de un servicio prestado a través de Internet y esta acción lleva asociado un cambio respecto del responsable del fichero que contiene los datos personales de los usuarios de ese servicio, tal acción puede comportar una cesión de datos. En este caso deberán observarse las previsiones legales y, en especial, la previa obtención del consentimiento de los usuarios, salvo que sea aplicable una excepción al mismo.

En el caso de que tal acción no comporte una cesión de datos, el nuevo responsable deberá informar convenientemente a los usuarios de modo expreso, preciso e inequívoco de su propia identidad y dirección, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. En este caso, tales datos sólo podrán ser utilizados por el nuevo responsable con las finalidades determinadas, explícitas y legítimas para las que hubieran sido obtenidos por el

anterior responsable.

4. Los usuarios serán convenientemente informados en los casos en los que sus datos vayan a ser comunicados a los responsables de otras webs que pudieran estar vinculadas (por ejemplo, mediante un hiperenlace) con la web a través de la cual son recogidos, siempre y cuando la comunicación se realice en los términos expresados por el apartado 1 de la presente Recomendación. En tales casos, se especificará claramente qué datos serán comunicados, así como la identidad y dirección de los cesionarios.

## OCTAVA: MOVIMIENTO INTERNACIONAL DE DATOS

1. De conformidad con lo establecido por el artículo 33 de la LOPD, 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 Ley Orgánica, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos.

A este respecto, se tendrán en cuenta las excepciones previstas en el artículo 34 de la LOPD:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

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

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.<sup>1</sup> En particular, cuando sea de aplicación la legislación española sobre protección de datos, conforme al artículo 2.1 de la LOPD, y además el fichero que contiene los datos personales recabados a través de Internet se halle ubicado en el territorio de un Estado no miembro de la Unión Europea o respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, será precisa la autorización previa del Director de la Agencia de Protección de Datos, a menos que la transferencia internacional se fundamente en alguno de las excepciones comprendidas en los apartados a) a j) del artículo 34 de la LOPD antes citados. En todo caso, la transferencia internacional se deberá

notificar a la Agencia de 1 Las decisiones de la Comisión Europea 2000/518/CE y 2000/519/CE, de 26 de junio, han considerado adecuado el nivel de protección de datos personales en Suiza y Hungría. Así mismo, la Decisión 2000/520/CE, de igual fecha, ha efectuado la misma declaración respecto de las empresas de los Estados Unidos de América acogidas al sistema de "puerto seguro".

Protección de Datos para su inscripción en el Registro General de Protección de Datos.

2. De acuerdo con lo que establece el artículo 5 de la LOPD y se recoge en la Norma Segunda de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.

3. El deber de información a que se refiere el apartado anterior no será de aplicación cuando la transferencia internacional tenga por objeto la prestación de un servicio al responsable del fichero, por parte de un tercero al que se le haya encargado el mismo en los términos establecidos por el artículo 12 de la LOPD.

4. Con independencia de lo anterior, en el caso de que la transferencia se legitime mediante la obtención del consentimiento inequívoco del afectado, el responsable del fichero se asegurará de que éste ha sido previamente informado de los extremos citados en el apartado 2.

#### **NOVENA: SEGURIDAD DE LOS DATOS**

1. De acuerdo con lo establecido por el artículo 9 de la LOPD, el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas en el Reglamento de Medidas de Seguridad, aprobado mediante el Real Decreto 994/1999, de 11 de junio, las cuales se clasifican de acuerdo a los niveles de seguridad establecidos en su artículo 4.

3. Cuando los usuarios registrados en una web tengan acceso on-line a los datos de que dispone el responsable del fichero respecto a su persona, deberán establecerse procedimientos de identificación, autenticación y control de accesos, de acuerdo con lo establecido en el citado Reglamento.

4. A los ficheros con datos acerca de transacciones de compra de productos o servicios que, mediante un tratamiento de segmentación o categorización, permitan obtener una evaluación de la personalidad del individuo, les será de aplicación, al menos, lo establecido en el apartado 4 del artículo 4 del citado Reglamento, es decir, en tal caso deberán de garantizarse las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20 del mismo.

5. Se considera una buena práctica la adopción de medidas que eviten que la información circule por la red de forma inteligible y, por tanto, susceptible de ser conocida o manipulada por terceros. Del mismo modo, se considera buena práctica proporcionar al usuario información acerca del nivel de protección que proporciona la tecnología utilizada.