EL TRATAMIENTO DE LOS DATOS PERSONALES EN INTERNET

Javier Domingo Ripalda

INDICE DE LA COMUNICACION

- ✓ ***introducción***. ***Objeto de la comunicación***.
- ✓ ***La figura del responsable del fichero en Internet. Obligaciones.***
- ✓ ***El correo electrónico como dato personal. Problemática.***
- ✓ ***Las cookies como datos de carácter personal. Problemática***.
- ✓ ***Deber de información en la recogida de los datos personales***. ***Especialidades en el otorgamiento del consentimiento***. ***El Encargado del Tratamiento***. ***Problemática y casos reales***.
- ✓ ***Conclusiones.***

INTRODUCCIÓN. *OBJETO DE LA COMUNICACIÓN*

Mediante el presente documento, se pretende dar una idea global y actual de las implicaciones que la aparición de Internet está suponiendo en la regulación referente a la recogida, tratamiento y cesión de los datos personales.

De ahí que, en el presente texto, nos encontremos una lógica contraposición entre las potencialidades que las Nuevas Tecnologías otorgan a los prestadores de servicios frente a las limitaciones y obligaciones que legalmente se están imponiendo con la finalidad de defender distintos derechos, entre los que se encuentra el derecho a la seguridad y la integridad de los datos personales.

Es evidente que el ordenamiento jurídico español ha sido dotado por el legislador de una legislación muy potente y exigente *(*Ley Orgánica de Protección de Datos y el Real Decreto 994/1.999 de Medidas de Seguridad) que obliga a los Responsables de los diferentes ficheros a cumplir una serie de obligaciones pero no menos importante es la idea que se pretende transmitir mediante el presente documento. Sin dejar al margen la necesidad de cumplir con dichas obligaciones legales, es necesario que exista una concienciación generalizada de que se debe establecer una política de seguridad (cada organización necesitará la suya propia) de forma que se establezcan unos mecanismos y procedimiento mediante los cuales se salvaguarden sus sistemas (en sentido amplio) y la información que éstos contengan.

Ello implica la aparición de una nueva rama estratégica dentro del mundo empresarial cuya finalidad será proteger y mantener la disponibilidad de los sistemas (sea cual sea el soporte utilizado) buscando un nivel homogéneo y coherente en el grado de seguridad que deba alcanzarse evitando la aparición de agujeros negros en determinados puntos del sistema.

LA FIGURA DEL RESPONSABLE DEL FICHERO EN INTERNET. OBLIGACIONES.

Comenzaré la presente exposición con el lema utilizado por la propia Agencia de Protección de Datos (en adelante, APD) de forma literal: "***evita que la informática invada tu intimidad***".

Es la propia LOPD la que define la figura del **Responsable del fichero** señalando que "es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Es decir, se trataría de cualquier empresa pública o privada, profesional independiente, Administración, ya sea estatal, autonómica o local y cualquier otro tipo de organismo que decida sobre un fichero que contenga datos personales.

Pero, ¿qué es un fichero que contenga datos personales? Literalmente la LOPD alcanza a los "***datos de carácter personal***" (cualquier información concerniente a personas físicas identificadas o identificables) "***recogidos en cualquier tipo de fichero***" (conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso)

Resulta curiosa la comparación entre el lema de la APD y el objeto de la LOPD. No sólo nos referimos a la informática como soporte de los datos personales sino a cualquiera de los soportes que puedan llegar a incluir datos personales. Ello nos lleva a concluir que una empresa o profesional podría no tener ningún tipo de sistema informático (utilizar sólo libretas, folios, notas) y estar afecto a la LOPD e, incluso, al R.D. 994/1.999 de Medidas de Seguridad.

Sin embargo, nos encontramos con que la presente comunicación hace referencia al mundo de Internet. A priori, las diferencias entre una empresa "tradicional" y otra que opere en la red son evidentes y ello permite establecer una serie de pequeñas pautas a la hora de cumplir con la legislación sobre Protección de datos.

De manera exhaustiva, y combinando las obligaciones establecidas tanto en la Ley Orgánica de Protección de Datos como en la Ley de la Sociedad de la Información (en adelante, LSSI) o Ley de comercio electrónico de reciente aprobación, resultaría que una organización que operara en Internet realizando cualquiera de las operaciones definidas como "**servicios de la sociedad de la información**" (contratación de bienes y servicios, suministro de información, actividades de intermediación, transmisión de datos por redes, alojamiento en servidores de información...etc) tendría que cumplir con las siguientes obligaciones impuestas por el Nuevo Derecho de las Tecnologías:

1. En virtud de la **LOPD** y del **Real Decreto de Medidas de Seguridad**, tendrá que efectuar las siguientes acciones:

    a. Caso de disponer de ficheros conteniendo datos personales (cosa realmente fácil si se vende por Internet, o si se tiene una revista on line que se envía a cuentas de correo electrónico, o si se reciben sugerencias

o quejas de los usuarios... etc) ***deberá notificarse su creación a la APD*** mediante los formularios habilitados legalmente.

b. En el caso de que se recaben datos personales mediante un formulario electrónico o cualquier otro tipo de medio electrónico (supuesto muy común en caso de compras de bienes o servicios o en caso de apuntarse a listas de distribución de noticias), ***deberá cumplirse con el deber de información*** expresado en el articulo 5 LOPD (cuestión que se detallará más adelante en otro apartado)
c. En caso de que se hiciera necesario, ***se necesitará obtener el consentimiento on line del titular de los datos personales*** tanto para el ***tratamiento*** como para la ***cesión*** de los datos personales (cuestión que se detallará más adelante en otro apartado)
d. Será necesario que la empresa cuente con un ***Documento de Seguridad*** donde se recojan las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.
   Como mínimo, esta política de seguridad supondrá una actuación constante en una serie de áreas: evaluación de los riesgos, protección perimétrica, control de acceso a los recursos, directrices en el uso de Internet y del correo electrónico, antivirus y copias de seguridad.
e. Directamente derivado de la anterior obligación, residirá la ***necesidad de que se implanten las medidas de seguridad en función de los niveles de seguridad*** que resulten aplicables a los diferentes ficheros (ya que de nada servirá un Documento de seguridad que se quede sin aplicación en la realidad)
f. De igual forma, deberá arbitrarse un ***procedimiento interno*** que permita que, de forma ágil los afectados puedan ***ejercer los derechos*** de acceso, rectificación, cancelación y oposición previstos en la LOPD.
g. Finalmente, tal y como señala el artículo 12 de la LOPD al referirse a la figura del ***Encargado del Tratamiento***, deberá regularse por escrito en un contrato u otro documento admitido en Derecho aquellas situaciones en las cuales cualquier tercero trate, directa o indirectamente, los datos personales por cuenta del Responsable del fichero (caso frecuentísimo en Internet si la web de un comerciante se aloja en un servidor de un proveedor de hosting ajeno o en el caso de que el servicio de atención al cliente se subcontrate con una empresa especializada...etc)

Dichas obligaciones que propone tanto la LOPD como el Reglamento de Medidas de Seguridad son muy ambiciosas. Realmente, estudios recientes (a los que se les podrá dar la fiabilidad que cada uno desee) otorgan un grado mínimo de cumplimiento de la legislación sobre Protección de Datos del 10% o incluso inferior.

Así, un estudio realizado por la empresa **Belt Ibérica, S.A.** señala que "*pese a que el plazo para ponerse al día respecto a la LOPD concluyó el pasado 26 de junio de 2.002 y pese a la mayor concienciación social en la materia- según la propia APD-* ***un 93% de las empresas no cumple correctamente con la normativa vigente***".

Si ese dato resulta alarmante, más si cabe resulta el dato recogido por las propias **Cámaras de Comercio** con fecha de 11 de junio del presente año (de nuevo, la fiabilidad del dato podrá resultar cuestionable a gusto de cada persona) según el cual "***sólo 167.147 empresas con actividad probada cumplen con la LOPD, lo que supone tan sólo el 5% del total***" (que, si los cálculos son correctos, supondría un número de 3.175.793 empresas infractoras)

Si considerásemos que estos estudios no resultan fiables, podríamos acudir a las propias **recomendaciones publicadas por la APD** y, concretamente, a la publicada en relación con el **sector del comercio electrónico** con fecha del último trimestre de 2.000.

Como una mera ejemplificicación, de un análisis de 44 webs que desarrollaban comercio electrónico, ***el 36% de los Responsables de los ficheros no se había inscrito en el Registro General de la APD***, ***el 27% no procedía a informar de lo dispuesto en el artículo 5 LOPD*** y ***el 46% no utilizaba el protocolo seguro HTTPS (SSL) para establecer un canal seguro de comunicación.***

De todos estos datos, se puede extraer una conclusión inicial: en este país, una vez transcurridos prácticamente tres años desde la aparición de la LOPD y una vez finalizados los plazos para implantar las medidas de seguridad, la mayor parte de las empresas no han adaptado su funcionamiento a las nuevas obligaciones legales impuestas en esta materia.

2. Adicionalmente, como consecuencia de la recientemente publicada **LSSI**, una empresa que operase en Internet deberá cumplir con otras obligaciones adicionales:

    a. En virtud del **artículo 9 LSSI**, los prestadores de servicios de la información deberán dejar una constancia registral del nombre de dominio o dirección de Internet que utilicen para identificarse.
    b. Según lo establecido en el **artículo 10 LSSI**, y sin perjuicio de los deberes de información que se establecen en la normativa vigente (parece que la LSSI se está acordando del artículo 5 LOPD), el prestador de servicios de la sociedad de la información facilitará a los usuarios y a los órganos competentes por vía electrónica la siguiente información: (***1***) su nombre y denominación social así como su residencia y domicilio, su dirección de correo electrónico y cualquier otro dato para poder entablar una relación directa (en este apartado, se produciría una duplicidad del contenido del deber de información con el artículo 5 LOPD si concurriese el hecho de tratarse de una empresa que opera en Internet como prestadora de servicios que tratase datos personales), (***2***) los datos de inscripción del dominio en el Registro Mercantil, (***3***) en caso de ejercicio de una profesión regulada, una serie de datos referentes a titulación, colegio profesional de adscripción y normas profesionales, (***4***) el número de identificación fiscal que corresponda, (***5***) información clara y exacta sobre precios, indicando si incluye o no los impuesto, y sobre los gastos de envío y (***6***) los códigos de conducta a los que se adhiera la empresa.

c. En caso de ser el Responsable del Fichero un prestador de servicios de intermediación (**artículo 11 LSSI**), si un órgano competente ordenase la interrupción de la prestación de dicho servicio o la retirada de contenidos provenientes de prestadores de servicios radicados en España, deberá colaborar en la suspensión de la transmisión, alojamiento de datos y el acceso a redes.
d. En caso de ser el Responsable de los ficheros tanto un operador de redes y servicios de comunicaciones, o un proveedor de acceso a redes de telecomunicaciones e incluso un prestador de servicios de alojamiento de datos (**artículo 12 LSSI**), deberá retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación del servicio durante un período máximo de doce meses.
e. Por último, aplicable a todo tipo de empresa opere o no en Internet, el legislador ha optado por prohibir el spam (**artículo 21 LSSI**) de forma que queda prohibido el envío de comunicaciones publicitarias o promocionales por mail si previamente no hubiesen sido solicitadas por los destinatarios de las mismas.

Cabe destacar que, en la actualidad, ***el 30% de las quejas que se presentan en la APD se refieren a un uso fraudulento de los datos en Internet*** (concretamente, el Director de la APD, Don Juan Manuel Fernández López, señaló con fecha de 14 de marzo de 2.002 que de 700 denuncias presentadas, 231 guardaban relación con Internet, principalmente con transacciones comerciales on line y bancos a distancia)

EL CORREO ELECTRÓNICO COMO DATO PERSONAL. PROBLEMATICA.

Supone hoy en día unos de los servicios más utilizados en Internet ya que permite la creación y transmisión de mensajes entre usuarios de la red sin que se requiera que estén conectados simultáneamente.

Sin embargo, no se garantiza que los mensajes lleguen siempre a su destino, ni que se informe de este hecho al remitente o que éste último sea quien dice ser.

Es necesario tener presente que la dirección de correo electrónico es la forma más habitual de registrar la identidad de una persona en Internet. En muchas ocasiones, contiene los datos de filiación de una personas, la razón social de su empresa o su propia nacionalidad. Esta dirección se puede llegar a usar en múltiples lugares de la red y se puede conseguir fácilmente sin nuestro conocimiento.

Su aspecto más preocupante se fundamenta en que pueda servir de base para la confección de perfiles personales (temas de interés, inclinaciones políticas o culturales o de ideología, orientación sexual) a partir de nuestra pertenencia a grupos de distribución o a grupos de discusión. En este caso, nos exponemos a que los datos proporcionados puedan ser recopilados sin informar al afectado y sin obtener su consentimiento utilizándolos para otros fines.

Dada la casuística que se puede llegar a producir, abordaremos unos casos concretos:

1. En caso de que se produzcan envíos de mails a clientes, proveedores, representantes, candidatos, operarios, etc. parecería recomendable cumplir con el deber de información del artículo 5 LOPD incluyendo una cláusula en el propio correo electrónico (de esta forma, conseguiremos una mayor seguridad como afectados al saber la procedencia de los datos y la identidad y dirección del Responsable del fichero)

2. Como ya se ha advertido con anterioridad, el spam o envío indiscriminado de mails conteniendo publicidad o promociones se prohíbe desde la aprobación de la LSSI (dejando claro que se prohíbe el spam realizado por empresas que radiquen en España o que tengan un establecimiento en el país)

   En este sentido, debe quedar claro que, si una empresa que opera en Internet desea mandar comunicaciones publicitarias electrónicas, deberá informar de ello al usuario obteniendo su consentimiento expreso (clickeando "aceptar" dentro de un campo expresamente preparado para ello), no siendo válidas aquellas cláusulas abusivas ("prácticamente escondidas" en diferentes links dentro del proceso normal de la contratación electrónica) que suponen un consentimiento no emitido expresamente.

   Por ello, en el Marketing on line, se restringe claramente la posibilidad de obtener datos personales (concretamente, el mail) de otra fuente que no sea el propio usuario. Sin embargo, las formas más habituales de obtener el correo sin el consentimiento del usuario son las listas de distribución, la captura de direcciones en directorios de correo electrónico, venta, alquiler o intercambio de direcciones por parte de proveedores de acceso y entrega de la dirección de correo por parte del navegador al conectarse al servidor web.

   Es decir, según la nueva legislación vigente, es imposible acudir a la compra de una base de datos compuesta por mails para su uso publicitario salvo que la empresa que gestionase dicha base de datos hubiese obtenido el consentimiento de los usuarios para, por un lado, ceder las direcciones de correo a terceros y, por otro, usar su dirección de correo con finalidades publicitarias.

3. Debe asumirse que el correo electrónico en Internet no es seguro a menos que se utilicen mecanismos de cifrado físico o lógico. Cuando se participa en foros de discusión o en listas de distribución, las informaciones vertidas son públicas y accesibles durante mucho tiempo, por lo que las opiniones pueden ser susceptibles de ser mal interpretadas o mal utilizadas.

LAS COOKIES COMO DATOS DE CARÁCTER PERSONAL. PROBLEMÁTICA.

Podemos definir una cookie como un conjunto de datos que envía un servidor web a cualquier navegador que le visita con información sobre la utilización que se ha hecho por parte de dicho navegador de las páginas del servidor, en cuanto a la dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. de forma que esta información se almacena en un fichero en el directorio del navegador para ser utilizada en una próxima visita a dicho servidor.

Ello implica que el comportamiento del consumidor o usuario en Internet puede ser "espiado" por el proveedor del servicio sin que se tenga conocimiento de ello ni se otorgue consentimiento al respecto.

Existen medios para evitar la recogida de estos datos personales y uno de los más importantes reside en la utilización de servidores que permiten navegar en Internet de forma anónima.

De esta forma, el sistema consiste en que el usuario accede, en primer lugar, a un servidor especializado en este cometido que le proporciona una identidad nueva a través de la cual puede acceder a otros servidores. De esta forma, los servidores web a los que se accede no podrán obtener la auténtica identidad del usuario.

Resulta evidente, por tanto, la cesión involuntaria que el usuario hace de sus datos personales por medio de la instalación de dichas cookies. Así mismo, existen otras conductas atípicas que suceden como supuestos reales al visitar una página ya que involuntariamente podemos llegar a ceder datos de todo tipo:

- ✓ Existen una serie de datos obtenibles con Java como pueden ser la dirección de correo electrónico (posible identidad del usuario), el tipo de navegador, la versión y el idioma, el sistema operativo, las fuentes instaladas, el nombre asignado al ordenador, la dirección IP (ya sea fija o dinámica), el número de páginas visitadas y la URL de procedencia.
- ✓ A su vez, pueden llegar a obtenerse una serie de datos con ActiveX y VB como podrían ser el historial de navegación, los datos del usuario, los datos referidos a otros programas y las direcciones de e-mail.

De esta manera, a efectos de evitar intromisiones no deseadas, existen medios para evitar estas cesiones de los datos personales mediante la activación del filtro de cookies y la configuración segura del navegador (aceptación previa de las cookies, bloqueo de java, Visual Basic y Actives, el bloqueo de la ejecución de programas, el filtro de contenidos activo, el bloqueo del envío automático de correo electrónico)

Si bien estos son medios que se encuentran al alcance de los usuarios, la línea iniciada en otros países europeos como Francia y Alemania ha supuesto que se regule el uso de las cookies preservando la privacidad de los usuarios. Varias líneas legislativas han procedido a regular la utilización de dichas cookies autorizándolas "únicamente si el usuario ha recibido previamente una información clara y completa sobre las finalidades del tratamiento y los medios de que dispone para oponerse a él", permitiéndose el uso de esos ficheros que "sólo sean empleados para facilitar las comunicaciones"

Pese a que el legislador español no ha regulado expresamente el tema de las cookies, contamos con el artículo 5 LOPD referido al deber de información como una posible solución a dicha carencia. Si se hiciese una interpretación extensiva del artículo y partimos del hecho de que la cookie captura datos de carácter personal que son conocidos por un proveedor de servicio, tenemos que concluir que ello supone la existencia de un fichero que contiene datos personales por lo que debería cumplirse con todas las obligaciones que el Responsable del fichero tiene (ya mencionadas con anterioridad) entre las que se encuentra el deber de información

del artículo 5 LOPD. De hecho, algunas compañías han incluido un aviso acerca de la colocación de cookies en el ordenador del usuario así como su finalidad, tal y como se prevé en el artículo 4 del Código Ético de Protección de Datos Personales de la AECE.

De esta forma, se cumple con el espíritu de la ley dado que la información recabada por este procedimiento no es facilitada voluntariamente por el ciudadano ni requiere la intervención de éste.

DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS PERSONALES. ESPECIALIDADES EN EL OTORGAMIENTO DEL CONSENTIMIENTO. ***EL ENCARGADO DEL TRATAMIENTO***. ***PROBLEMÁTICA Y CASOS REALES***.

En relación con estos dos apartados, cabe destacarse que, ya la APD en el año 2.000 dentro de las recomendaciones al sector del comercio electrónico, era durísima al destacar que una de las carencias más importantes que se observan en las webs dedicadas al sector del comercio electrónico era 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) A la propia APD le parecía significativo que el 27% de las webs que analizó no cumplían en ningún momento con este **deber de información del artículo 5 LOPD** mientras que opinaba que el resto de las webs sí que incluía un texto con el que la APD "entendía" que se pretende cubrir en mejor o peor medida ese requisito legal.

Han pasado dos años desde estas recomendaciones y muchas páginas webs (no sólo las que se dedican al comercio electrónico en sentido estricto de venta de productos o de servicios sino cualquier tipo de web en la que se recaben datos personales) no cumplen con este deber de información al recabar en numerosos formularios los datos personales de los afectados (por ejemplo, introducción de un currículum vitae on line, buzón de sugerencias de mejoras de la web, inclusión en una lista de correo para el envío de noticias en una web especializada..etc)

Si grave es no informar, más aún parece el hecho de hacerlo de forma deficiente ya que puede ocultarse datos de tanta importancia como quien es el Responsable del fichero o del tratamiento, lo cual es especialmente grave cuando se accede a una determinada página a través de un hiperenlace.

Sin duda alguna, lo realmente destacable en el mundo de Internet respecto del mundo de la empresa tradicional se basa en que, en muchas ocasiones, resulta complicado para el usuario distinguir claramente la figura del comerciante (con quien realmente el adquirente desea mantener una relación o transacción comercial) de las figuras de los meros intermediarios (que ponen en contacto a ambos y que pueden llegar a convertirse en Encargados de Tratamiento)

El usuario de Internet debería ser consciente de que, una vez facilitados sus datos personales, estos pueden pasar por las manos de los diferentes intervinientes en un proceso de venta on line: aquel que gestiona el servidor web por cuenta del comerciante, el que puede autorizar la transacción financiera, el propio comerciante,

el que emite los documentos que acreditan la titularidad de un producto o servicio, el que se encarga de la logística de la venta, el que realiza el servicio hot-line de atención al cliente o el servicio post-venta. Como en los casos más habituales no suelen coincidir estas figuras en una misma entidad, es importante que el comprador sepa quien decidirá finalmente sobre el uso y finalidad de los datos personales.

Por ello, en todas y cada una de las páginas web en las que se proceda a recabar datos personales, se incluirá la información establecida en el artículo 5 LOPD que el usuario podrá obtener fácilmente, de forma rápida y sencilla.

Además, lo más recomendado es que la lectura de dicha información sea un paso ineludible dentro del transito de acciones que el usuario debe realizar anteriormente a la aceptación de la transmisión definitiva de los datos a la entidad correspondiente.

Dicho deber de información contendrá, como mínimo, los siguientes extremos: (***a***) la existencia de un fichero, la finalidad de la recogida de los datos y de los destinatarios de la información, (***b***) el carácter facultativo u obligatorio a las preguntas que les sean planteadas, (***c***) las consecuencias de la obtención de los datos o de la negativa a suministrarlos, (***d***) la posibilidad de ejercitar los derechos reconocidos en la LOPD y (***e***) la identidad y dirección del Responsable del tratamiento.

De manera reciente, la propia APD ha iniciado una investigación a efectos de poder comprobar el uso y finalidades que se está dando del tratamiento de los datos personales recogidos mediante el novedoso sistema de votación vía teléfono (ya sea teléfonos móviles mediante los mensajes SMS o fijo) debido a las denuncias de usuarios que desconocían que uso y finalidad se les daba.

Otro tema diferente es el que se da en el **otorgamiento del consentimiento** por parte de los usuarios. La ley distingue claramente dos tipo de consentimientos: el que se otorga para efectuar la recogida y el tratamiento de datos personales por parte de una entidad y el que se puede otorgar para que dicha entidad pueda ceder esos datos personales a un tercero.

De manera general, ***el tratamiento de los datos personales*** requerirá el consentimiento inequívoco del afectado, salvo que la ley prevea otra cosa o se puedan aplicar las excepciones de la LOPD (es básica la excepción del artículo 6.2 referida a que los datos se refieran a las partes de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento)

Por ello, debe quedar claro que 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 entiende que consiente siempre de acuerdo a los extremos de los que haya sido conveniente informado. De aquí, se puede visualizar la relación tan íntima que tiene el cumplimiento del deber de información del artículo 5 LOPD con el consentimiento informado que un usuario de Internet puede llegar a emitir. Por supuesto, si el usuario revoca un consentimiento, el Responsable del tratamiento debe habilitar los medio para que se excluya el tratamiento de los datos.

Sin embargo, dentro de la LOPD nos encontramos con un determinado tipo de datos de carácter personal que se definen como "datos especialmente protegidos". Un primer tipo de datos son los que hacen referencia a los datos sobre ideología, afiliación sindical, religión o creencias que sólo podrán ser recogidos con consentimiento ***expreso y por escrito***. Una segunda modalidad de datos protegidos son los que hacen referencia al origen racial, a la salud y a la vida sexual que sólo podrán ser recabados, tratados y cedidos cuando así lo señale una ley por razones de interés general o el afectado haya ***consentido expresamente*** (aquí la LOPD no dice "y por escrito")

Por ello, la aplicación práctica al mundo de Internet de esta especial normativa de obtención del consentimiento la podemos encontrar en determinadas páginas que ofrecen la venta de productos orientados a las prácticas sexuales o a la venta de productos de tipo farmacéutico.

La recogida de determinados datos podría dar lugar a la obtención de un conjunto de datos personales suficientes para obtener una evaluación de la personalidad del individuo (más si cabe si se obtiene información del usuario sin que éste conozca que la cede) relacionada con su vida sexual o su salud. En tales casos, será necesario el consentimiento expreso del individuo mediante un procedimiento informático establecido que obligue a que el usuario tenga una participación activa.

Otra cuestión completamente diferente es la necesidad de la ***obtención del consentimiento*** para la ***cesión de los datos personales***. Este es un tema enormemente grave al tratarse su omisión como una conducta sometida a infracción muy grave por la LOPD y sancionada con multas que van desde los 30.050,60 euros hasta los 601.012,10 euros.

No sólo se trata de un tema grave el hecho de que los datos personales se cedan sin consentimiento de los afectados, o que se cedan para una finalidad no conocida o distinta para la que se señaló, o que se cedan a terceros no reconocidos sino que más grave aún es el hecho de que se cedan involuntaria o inconscientemente a un potencial y abstracto grupo de individuos (la red en Internet o las propias personas en la calle, por ejemplo) como consecuencia del incumplimiento del deber de seguridad por parte del Responsable del fichero (artículo 9 LOPD)

Casos recientes demuestran que es precisamente el incumplimiento de elementales medidas de seguridad (las que obliga a tener en cuenta el artículo 9 LOPD en relación con el Real Decreto de Medidas de Seguridad) las que han provocado cesiones de datos a determinados individuos extraños al afectado y sin que éste conozca dicha cesión hasta que se produce la denuncia pública.

Son casos, además, de gran importancia por el tipo de datos cedidos o perdidos involuntariamente como sucedió tanto en el caso de una cadena de supermercados en Madrid "*al tirar a la basura los currículum vitae de los candidatos a un puesto de trabajo en la empresa*" (noticia de 10 de julio de 2.002) como en el caso de "*la aparición de 7.000 expedientes médicos confidenciales dentro de unas bolsas de basura al lado de un contenedor pertenecientes a un centro médico andaluz con datos de salud de nivel alto de seguridad*" (noticia de 29 de julio de 2.002)

En este apartado, la LOPD es extremadamente clara al señalar que los datos de carácter personal sólo podrán ser comunicados a un tercero para el cumplimiento de los fines relacionados con las funciones legítimas del cedente y cesionario, ***previo consentimiento del usuario afectado***.

Es tan nítido este criterio legal que la APD no ha dudado en prohibir a las instituciones públicas de la CC.AA. de Madrid la cesión de los datos de las nóminas de los trabajadores de la Comunidad Autónoma a las asociaciones sindicales, salvo que exista consentimiento expreso del afectado (colisionando, en este caso, los derechos que concede la LOPD y los que concede el Estatuto de los Trabajadores)

Igual que ocurría con la necesidad del consentimiento para la recogida y tratamiento de los datos, existen excepciones a la necesidad del consentimiento para la cesión (de nuevo, que lo prevea una ley está entre ellas lo que ampara las cesiones de datos típicas por normativa legal, ya sea laboral, fiscal, contable o mercantil) siendo la más importante desde el punto de vista de la práctica contractual la situación en la que el tratamiento responda a la aceptación de una relación jurídica que implique la conexión de dicho fichero con ficheros de terceros (***la cesión será legal siempre que se limite a la finalidad que la justifica y no otra***)

Un caso en los que no se produjo este último requisito lo encontramos en el supuesto que aconteció en el año 2.001 en la Universidad de Zaragoza al cederse datos de los alumnos a terceras entidades, sin su consentimiento en ocasiones e, incluso, sin que los alumnos supieran que otro tipo de datos diferentes de los que habían consentido iban a ser comunicados a terceros (con lo que la finalidad de la cesión de datos que justificaba la cesión quedaba distorsionada)

En ese caso, tal y como señala la LOPD, el consentimiento para la cesión de los datos personales será nulo cuando la información que se facilite al afectado no le permita conocer la finalidad a la que se destinan los datos o el tipo de actividad del tercero al que se le vayan a comunicar.

En este sentido, es habitual que los datos recabados en Internet se comuniquen a otras compañías (siendo muy habitual que se traten de compañías de un mismo grupo de empresas) por lo que deberá comunicarse al usuario de forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos. La APD señala la necesidad de nombrar a dichas compañías con su denominación social (permite conocer o inferir cual es su actividad societaria), no siendo válida la coletilla tan recurrente que literalmente señala que “los datos serán cedidos a otras empresas del grupo para el envío de información publicitaria”.

Casos en los que se ha producido cesiones de datos entre empresas de un grupo sin el consentimiento del afectado son reiterados en nuestro país, siendo evidente en el caso de compañías de telecomunicaciones que proceden a intercambiar datos de sus clientes sin su consentimiento ***expreso*** (no lo olvidemos ya que una cosa es el consentimiento expreso que implica una acción positiva por parte del usuario y otra diferente es el consentimiento obtenido por defecto o de manera tácita al presuponer el consentimiento expreso en los usuarios) dando una finalidad a los datos completamente diferente a aquella para la que fueron recabados.

Por último, una de las figuras que aparecen constantemente en el mundo de Internet y que regula la LOPD es la figura del **Encargado del tratamiento**.

Ya se ha señalado con anterioridad que el usuario de Internet debería ser consciente que, una vez facilitados sus datos personales, estos pueden pasar por las manos de los diferentes intervinientes en un proceso de venta on line.

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 empresas más especializadas las tareas referidas a la atención telefónica, la logística o los servicios informáticos.

En estos tres supuestos, se produce el acceso a los datos personales de los clientes por parte de las empresas contratadas por lo que, en los tres casos será de aplicación lo previsto en el ***artículo 12 LOPD***.

Dicha regulación señala que ***el tratamiento de los datos personales por cuenta de terceros deberá estar regulada en un contrato*** que deberá constar por ***escrito***, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del tratamiento, que no los aplicará con un fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. Además de ello, en el citado contrato se estipularán las medidas de seguridad a que se refiere el artículo 9 LOPD que el encargado del tratamiento está obligado a implementar.

Parece evidente que dicho contrato intenta proteger al Responsable del fichero en caso de que el encargado incumpla cualquiera de las disposiciones en el mismo contenidas que, sin ir más lejos, no son más que las mismas obligaciones legales que se imponen a cualquiera que trate datos personales (implantación de medidas de seguridad en el tratamiento, cumplimiento de la finalidad definida contractualmente e imposibilidad de la cesión de los datos)

Adicionalmente, 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 el que conste algún dato de carácter personal objeto del tratamiento.

Como consecuencia de las inspecciones realizadas en su momento por la APD en su inspección al sector del comercio electrónico del último trimestre del año 2.000, se pudo destacar que no siempre se atendía adecuadamente a este requisito legal. Existían documentos contractuales en los que se incluía una estipulación especial relativa a la confidencialidad de los datos, con la que se quería cubrir esta exigencia legal.

De igual modo, la realidad nos muestra que los servicios informáticos en el mundo de Internet suelen ser prestados por empresas extranjeras que utilizan documentos-tipo redactados por ellas mismas y que no recogen absolutamente nada de lo dispuesto en la normativa legal.

CONCLUSIONES.

Cabe resaltar que España tiene una de las legislaciones en materia de protección de datos más duras y ambiciosas de todo el panorama jurídico continental e, incluso, mundial. Sin embargo, y sin que ello suponga una contradicción, **una mirada crítica de la realidad nos llevaría a concluir que existe un trecho entre lo que existe y lo que debería existir en materia de protección de datos**.

Tal y como se ha señalado en la comunicación, el hecho de que la ley afecte tanto a una base de datos con la que se haga data mining como a una ficha de proveedor nos lleva a una situación en la que prácticamente cualquiera que desarrolle una actividad, del tipo que sea, debe cumplir con la legislación vigente.

Esta situación, lejos de ser preocupante, debe concienciarnos del adelanto legislativo español en materia de protección de este derecho constitucional pero, al mismo tiempo, debe hacer reflexionar sobre la imposibilidad de un cumplimiento completo de todas las obligaciones.

Esta legislación tan ambiciosa – a veces, imprecisa en sus definiciones técnicas- supone, en ocasiones, la imposibilidad de su cumplimiento. Sería mucho más correcta una gradación en los niveles de cumplimiento de la legislación (no es posible comparar la base de datos y el sistema informático de un centro médico o de un portal de Internet con varios millones de usuarios inscritos con el software de nóminas estandarizado de una PYME en el que tan sólo se contiene un dato personal sensible como es el grado de minusvalía para el cumplimiento de la obligación fiscal de retener) y que los órganos encargados de su cumplimiento fuesen dotados de mayores y mejores recursos para conseguir una óptima labor fiscalizadora.

Adicionalmente, el cumplimiento se complica por el hecho de que la legislación impone unas obligaciones legales y técnicas que no están al alcance (no sólo económico sino técnico) de la mayor parte del tejido empresarial español.

Sin embargo, mayor preocupación demuestra el hecho de que ni siquiera algo tan evidente y fácil de realizar como es la inscripción de los ficheros en el Registro General de la Agencia de Protección de Datos se efectúe. Ello creo que puede demostrar que existe un mayor fallo que las propias características de la legislación: **su desconocimiento generalizado** (que incluye, claro, las sanciones)

Como consecuencia, el cumplimiento de la legislación es más avanzado en las grandes organizaciones con mayores recursos y menor en las más pequeñas. Ello implica que las entidades que no adopten las medidas de seguridad están asumiendo el riesgo de un ataque externo e interno de seguridad pero también de una potencial sanción. Y, de aquí, surge una pregunta que queda formulada de la siguiente manera: ¿qué actitud debería tomar un auditor de cuentas que detectase estos riesgos (cuantificables económicamente por la tabla de sanciones de la LOPD, no lo olvidemos) a la hora de realizar un informe de auditoria?¿debería dejar clara una salvedad en su informe aconsejando dotar una provisión por el riesgo de ser sancionado por la APD en caso de una denuncia?