La protección de datos personales en Internet

(Protection of personal data on the Internet)

Chaveli Donet, Eduard
Eusko Ikaskuntza. Miramar Jauregia. Miraconcha, 48.
20007 Donostia – San Sebastián

BIBLID [1138-8552 (2008), 20; 83-100]
Recep.: 01.09.04
Acep.: 17.10.08

El artículo trata sobre los principales problemas prácticos que plantea la adecuación de un website a la LOPD así la dirección IP, el correo electrónico, los cookies… y su conceptuación o no como datos personales, las especialidades que la LOPD impone a las empresas que operan en Internet y las transferencias internacionales de datos.

Palabras Clave: Protección de datos de carácter personal en Internet. Websites. Dirección IP y dato personal. Correo electrónico y dato personal. Cookies y dato personal. Transferencias internacionales de datos.

Web gune bat Datuak Babesteko Lege Organikoari (LOPD) egokitzeko sortzen diren arazo praktiko nagusiak ditu hizpide artikuluak, hala nola IP helbidea, posta elektronikoa, kukiak… eta horiek datu pertsonalen kontzeptuaren barruan sartzen diren ala ez erabakitzea. Halaber, LOPDk Interneten diharduten enpresei inposatzen dizkien betekizunak eta datuen nazioarteko transferentziak ere aztergai ditu.

Giltza-Hitzak: Interneten datu pertsonalak babestea. Web guneak. IP helbidea eta datu pertsonalak. Posta elektronikoa eta datu pertsonalak. Kukiak eta datu pertsonalak. Datuen nazioarteko transferentzia.

L'article aborde les principaux problèmes pratiques découlant de l'adaptation à la LOPD (Loi de Protection des Données) d'un site web, tels que l'adresse IP, le courrier électronique, les cookies… et leur considération ou pas comme données personnelles, les exigences requises par la LOPD aux entreprises opérant sur Internet et le transfert de données sur le plan international.

Mots Clé : Protection des données personnelles sur Internet. Sites web. Adresse IP et données personnelles. Courrier électronique et données personnelles. Cookies et données personnelles. Transfert de données sur le plan international.

INTRODUCCIÓN[1]

Hace apenas dos años escribía una monografía bajo el título *El tratamiento de datos personales en el sector de los servicios de la sociedad de la información y el comercio electrónico*[2] y aunque este artículo sigue, en parte, la misma estructura que aquél, ese paralelismo sirve para evidenciar (como consecuencia de la comparación) lo que se ha avanzado en este tiempo: mucho en algunas cuestiones y nada en otras. Pero además, el presente artículo supone una actualización de los contenidos derivada no sólo de tales cambios normativos[3] sino también del posicionamiento que en algunos aspectos ha hecho público la Agencia Española de Protección de Datos (en adelante AEPD) y –también, hay que reconocerlo– de algún cambio de criterio propio.

El objetivo del presente artículo lo constituye el ofrecer una visión práctica y actualizada en la que se aborden –principalmente– las siguientes cuestiones: la conceptuación o no de determinados signos utilizados en Internet como datos de carácter personal; los principales servicios de la sociedad de la información con incidencia en la protección de datos, así como las peculiaridades que la Trasferencia Internacional de Datos supone al aplicarla a Internet.

1. CONCEPTUACIÓN O NO DE DETERMINADOS SIGNOS IDENTIFICATIVOS UTILIZADOS EN INTERNET COMO DATOS DE CARÁCTER PERSONAL Y PROBLEMAS QUE PRESENTAN

Para poder tratar la incidencia de la protección de datos en determinados servicios de la sociedad de la información es necesario plantearse previamente la conceptuación de algunos signos identificativos utilizados en Internet como dato de carácter personal. A ello dedicamos las siguientes líneas.

---

1. El autor quiere destacar que el presente artículo refleja el estado de la materia en la fecha en que se realizó la conferencia de la que el mismo es consecuencia y que desde entonces: se han producido numerosos e importantes cambios legislativos en la materia y ha habido pronunciamientos por parte de la Agencia Española de Protección de Datos y de los Tribunales que hacen que algunas de las consideraciones que en el mismo se realizan sean total o parcialmente inaplicables a fecha de hoy.

2. *El tratamiento de datos personales en el sector de los servicios de la sociedad de la información y el comercio electrónico,* monografía realizada por Chaveli Donet, E. y Picazo Sentí, P., y publicada en www.vlex.com.

3. Tengamos en cuenta que en poco tiempo desde la entrada en vigor de la LSSI se han producido ya sendas modificaciones de la misma: las efectuadas por el artículo 1.1. de la LGT (Ley 32/2003, de 3 de noviembre. Disposición Adicional 1ª) y la que contempla la Ley de Firma Electrónica (Ley 59/2003, de 19 de diciembre, Disposición Adicional 8ª).

1.1. La dirección IP

La dirección IP (acrónimo de Internet Protocol) es un número único que usan los ordenadores para identificarse entre ellos. Todo ordenador que está en línea tiene una dirección IP. Consta de cuatro series de números enteros entre 0 y 255. Un ejemplo de dirección IP sería 194.98.200.23.

Aparte de otras clasificaciones que no interesan ahora, las direcciones IP pueden ser dinámicas o fijas[4]. El uso de la dirección IP es necesario dado que, como hemos mencionado, los ordenadores la emplean para identificarse al conectarse a la red, enviar un correo, etc.[5].

De un correo electrónico que nos remitan podemos extraer, entre otras cosas y a los efectos que aquí nos interesan, la dirección IP del ordenador desde el que se remite. También aparecen otros datos identificativos (como el remitente y su correo) que, asociados a la IP, pueden convertir esta información en futuras operaciones en un dato de carácter personal. Si bien esta utilización de la IP como identificadora del origen del correo puede reputarse normal, en principio, los posteriores usos que se hagan de la misma una vez asociada a un dato personal pueden no serlo tanto.

También el uso de la IP es, en ocasiones, normal y necesario en los servicios de navegación a través de la www[6]. En este escenario lo habitual es que el registro de la dirección IP sirva para fines "normales" como son las estadísticas de acceso a determinados *sites* y no para otros que plantean mayores problemas en materia de protección de datos, como pueda ser deducir "hábitos" de navegación. Pero no siempre es así. Ello nos obliga a abordar la posible conceptuación de la IP como dato de carácter personal.

---

4. Si una dirección IP es dinámica, se asigna automáticamente al ordenador con base a una reserva de números disponibles cuando el mismo se conecta a Internet o a la red local. Esto significa que el ordenador tendrá una dirección IP distinta cada vez que se use Internet, y podrá utilizarse únicamente para identificar la red o al Proveedor de Servicios de Internet que sea el propietario de la reserva de direcciones de la que se tomó la dirección que se asignó al ordenador. Si una dirección IP es fija, el usuario o el administrador de la red debió introducir manualmente una dirección IP a su ordenador cuando se activó por primera vez su acceso a Internet. En este caso la dirección IP será la misma cada vez que el usuario se conecte a Internet o a su red local, y podrá utilizarse para identificar el ordenador.

5. Para facilitar la comprensión del concepto, generalmente se utiliza el siguiente ejemplo: si queremos visitar una página web realmente lo que estamos haciendo es que nuestro ordenador (que es el cliente) le pida al servidor (camarero) que nos sirva algo (un correo, una web); pero para que el servidor nos lo envíe deberá conocer el número de nuestra mesa, es decir: nuestra dirección, nuestra IP.

6. La World Wide Web (WWW, WEB o W3) que para muchos se identifica con Internet es, en realidad, sólo una parte de esta. Estrictamente la WWW es la parte de Internet a la que accedemos a través del protocolo *HTTP*, y en consecuencia gracias a navegadores, siendo los más conocidos Netscape o Internet Explorer.

En este sentido Reyes Corripio[7] afirma que "la dirección IP no es la dirección de una persona física sino "la dirección red" de la máquina de un usuario conectado a Internet". Por tanto, la misma "no es, pues, un dato directamente personal", aun cuando sí puede serlo indirectamente.

Si bien me parece correcta esta conclusión, no comparto alguno de los argumentos en los que se fundamenta. En apoyo de esa tesis, cita una Sentencia del Tribunal Supremo, de 23 de marzo de 1993, donde se estima que la publicación de un anuncio ofreciendo servicios sexuales con un número de teléfono de una persona física puede lesionar su honor pues "facilitar el número de un abonado telefónico lleva consigo la posibilidad de su posterior determinación personal".

A mi entender tales argumentos no son aplicables a la dirección IP porque existe una diferencia muy importante entre ésta y la identificación telefónica: la identificación telefónica, al estar generalmente disponible en una fuente de acceso público, permite la identificación del interesado relacionando el número de teléfono con una persona determinada –mediante una búsqueda inversa, algo relativamente sencillo en la actualidad–; por el contrario, la titularidad de las direcciones IP no se contiene en fuentes de acceso público, por lo que ese segundo paso (relacionar la dirección IP con algún dato que identifique al usuario), que nos conduciría a la identificación de la persona, no es posible, en principio.

Por ello entiendo que la dirección IP únicamente, en sí misma, sin que pueda asociarse a otra información, no constituye un dato de carácter personal. Sí lo constituirá, sin embargo, desde el momento en que el usuario haya comunicado determinada información y sea posible, a partir de entonces, relacionar su dirección IP con el mismo. Estos supuestos, que suelen ser frecuentes en Internet, permiten cruzar la dirección IP con datos que sí identifican al usuario.

Por su parte la AEPD en su informe 327/03 concluye que

> aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos.

Entiendo que se trata de una conclusión errónea por ser demasiado generalizada ya que si bien es cierto que en determinados supuestos que se citan en el

7. Dª. Mª de los Reyes Corripio Gil-Delgado, en su obra "Regulación Jurídica de los Tratamientos de Datos Personales realizado por el Sector Privado en Internet" –premio *Protección de Datos Personales del año 2000*–, publicado en la *Memoria de la Agencia de Protección de Datos del año 2000.*

informe nos hallamos ante claros ejemplos en los que la IP constituye un dato de carácter personal[8], no es menos cierto que habrá que estar al caso concreto ya que –como la propia AEPD reconoce indirectamente– hay supuestos en los que la IP no constituye *per se* un dato de carácter personal[9].

1.2. El correo electrónico

Huyendo de otras definiciones eminentemente técnicas, a fin de centrar el estudio del concepto desde el punto de vista pretendido, basta señalar que el correo electrónico es un servicio de mensajería entre usuarios que, mediante la conexión a Internet, permite el envío y la recepción de mensajes de texto, imágenes, datos o mensajes de voz.

Es frecuente escuchar en algunos foros especializados la alusión a una supuesta diferencia de naturaleza entre el correo electrónico y el correo ordinario, apelando a una mayor transparencia –se dice– del primero. Ello se debe –sostienen– a que en el correo tradicional la identidad del remitente puede permanecer oculta, mientras que en el electrónico no. Coincidimos, en este punto, con lo afirmado por Reyes Corripio[10]:

> El correo electrónico lleva aparejada de por sí la transmisión de la dirección IP, ..., por lo que su utilización puede ser fuente de información personal identificable... Podríamos, en este sentido, equipararla con la dirección del remitente de un mensaje ordinario.

Ahora bien, ello será posible siempre y cuando la dirección IP sea fija, conforme a la clasificación realizada anteriormente.

---

8. "... A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha la hora y la duración de la asignación de dirección. Es mas, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación... en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación".

9. "...En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo"... habría que extender la misma consideración en relación con la IP fija, pues esta no es accesible tampoco – en principio – para todos.

10. Vid. obra citada "Regulación Jurídica de los Tratamientos ..." pag. 15.

Sin embargo, a mi entender y desde un punto de vista estrictamente jurídico, la dirección de correo electrónico es equivalente a la dirección postal, y así debe ser considerada a todos los efectos[11].

La dirección de correo electrónico viene configurada por dos parámetros: el login, generalmente escogido por el usuario; y el nombre de dominio, designado por la empresa que presta el servicio de correo electrónico.

Las posibilidades de configuración del login son numerosas: nombres propios, iniciales, números, nombres genéricos, combinaciones alfanuméricas... con la única limitación de que no coincida con otro preexistente en el mismo dominio que presta el servicio de correo. Dependiendo de la opción elegida por el usuario, encontramos direcciones que permiten identificar al mismo, y otras que, sin embargo, impiden –en principio– establecer relación alguna con su titular.

Habida cuenta de la definición de dato de carácter personal establecida en el artículo 3.a de la LOPD, (*cualquier información concerniente a personas físicas, identificadas o identificables)*, no cabe duda de que cuando la dirección de correo electrónico (tenga en sí misma o no un dato de carácter personal) se asocia a otro tipo de información personal (nombre, apellidos, dirección postal, etc.) constituye un dato de carácter personal. Es, sin embargo, más confuso, el supuesto en que únicamente se disponga de una relación de direcciones de correo electrónico. Este supuesto requiere analizar si la dirección de correo electrónico, en sí misma, constituye un dato de carácter personal. La AEPD, en un informe relativo a la cesión de direcciones de correo electrónico, ha manifestado su criterio con varios ejemplos:

El primero de ellos referido a aquellos supuestos en que la dirección de correo electrónico

> contenga información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado).

Según la AEPD

> en este supuesto, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso dicha dirección ha de ser considerada como dato de carácter personal[12].

---

11. Esto tiene especial importancia no sólo en relación con la conceptuación del correo electrónico como dato de carácter personal sino también (y especialmente) en relación con los problemas derivados del control del correo electrónico (problema que se plantea especialmente en el ámbito laboral y sobre el que existen algunos pronunicamientos judiciales.

12. Según la AEPD: "Ejemplos característicos de este supuesto serían aquellos en los que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel con el propio del país en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso así delimitarse el centro de trabajo en que se realiza la prestación".

Un segundo supuesto sería aquel en que, en principio,

> la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta[13].

En este caso, según la AEPD,

> Un primer examen de este dato podría hacer concluir que no nos encontramos ante un dato de carácter personal. Sin embargo, incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación. Por todo ello se considera que también en este caso, y en aras a asegurar, en los términos establecidos por la Jurisprudencia de nuestro Tribunal Constitucional, la máxima garantía de los Derechos Fundamentales de las personas, entre los que se encuentra el derecho a la "privacidad", consagrado por el artículo 18.4 de la Constitución, será necesario que la dirección de correo electrónico, en las circunstancias expuestas, se encuentre amparada por el régimen establecido en la LOPD.

A mi entender el primer supuesto se trata de un claro ejemplo en el que debe conceptuarse el correo electrónico como dato de carácter personal, aun cuando en algunos casos (en el supuesto de correos asociados a dominios abiertos[14]) puede ser que la identidad de la persona identificada no sea "real". Pero la consideración, en el segundo supuesto, del correo electrónico como dato de carácter personal, en términos generales, es –a mi entender– errónea. Se trata de un supuesto idéntico a la IP y, por tanto, la conclusión a la que se ha de llegar es la misma: en tales supuestos el correo electrónico será un dato de carácter personal en tanto en cuanto permita identificar a una persona. Y –siempre según mi entender– esta cuestión no es tan simple como pueda deducirse de la simple referencia –como se dice en el informe– a una simple "consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado".

1.3. Las cookies

Las cookies son ficheros de texto que un servidor almacena en el disco duro del ordenador del usuario, recolectando información relativa al mismo. El contenido de la información extraída dependerá del uso que el titular del website haya

13. Según la AEPD: "por ejemplo, el código de la cuenta de correo a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno".

14. Denominamos "correos asociados a dominios abiertos" a aquellos en los que el titular del dominio permite la elección de correos electrónicos asociados a dicho dominio sin verificar que existe una relación lógica (de buena fe) entre el login elegido y su identidad.

conferido a las cookies, pudiendo ser más o menos respetuoso con la privacidad de los consumidores.

La relación de las cookies con la privacidad se remonta a su misma existencia. En efecto, la posibilidad de las cookies de instalarse en el ordenador del usuario sin el conocimiento ni aprobación del usuario es uno de los puntos más controvertidos generados por su utilización, ya que es considerado como una trasgresión de la intimidad del usuario.

Y aunque es cierto que cabe la posibilidad de configurar el navegador del equipo informático de modo que o bien rechace las cookies automáticamente, o bien nos solicite aprobación cada vez que un servidor pretende la instalación de estos archivos en nuestro disco duro, no es menos cierto que esta opción puede llegar a entorpecer sobremanera la navegación, amén de no permitir cargar numerosas páginas en las que la aceptación de la cookie es necesaria para poder proceder a su visionado.

No obstante lo anterior, el uso de las cookies es una realidad y su convivencia con la normativa sobre protección de datos es posible. Para ello habrá que tener en cuenta, entre otras cosas, las Recomendaciones publicadas por la AEPD al sector del comercio electrónico. En ellas se dice que es importante que en la política de privacidad se informe al usuario de si el uso de las cookies es necesario o no para disfrutar de los servicios ofrecidos en la web y, por tanto, si tiene la posibilidad de configurar su navegador para que no las reciba.

Pero si la anterior información es conveniente, es necesario –siguiendo las mismas recomendaciones– que la Política de Privacidad recoja la finalidad del uso al que va a destinarse la información recogida por las cookies, a fin que el usuario pueda aceptarlo libremente. Un uso frecuente de las cookies lo supone cuando son empleadas a fin de facilitar una mejor navegación al usuario dentro de una web: personalizando el *site*, de modo que la siguiente vez que lo visitemos podamos acceder directamente a las áreas por las que hemos mostrado interés, o personalizando los anuncios existentes en la web –no mostrando el mismo anuncio que hemos visionado con anterioridad, o adaptando éstos a nuestros gustos y preferencias–. La AEPD no se muestra contraria a esta utilización, siempre y cuando la misma sea conocida y consentida por el usuario. Otro uso frecuente suele ir ligado al acceso a áreas o servicios reservados. Esto puede plantear algunos problemas, principalmente cuando la conexión se realiza mediante equipos de uso compartido, al facilitarse el acceso a información de otros usuarios del mismo equipo, lo que conlleva la posibilidad de acceder a las contraseñas almacenadas descifrando las cookies que se implantan en el disco duro del ordenador, lo que permitiría también la suplantación de la identidad de sus usuarios.

Probablemente por ello, las Recomendaciones de la AEPD al sector del comercio electrónico establecen la obligación de informar al interesado, de modo previo al comienzo de su empleo, de la existencia de procedimientos invisibles de recogida de datos (cookies, datos de navegación, contenidos activos...), uti-

lizados para recoger datos sobre su navegación e identidad. También se le deberá informar del nombre de dominio del servidor que activa los mismos, de su finalidad y plazo de validez, así como de la necesidad de aceptar estos procedimientos para visitar el sitio web y de la opción de que dispone de oponerse a esta modalidad de tratamiento, además de las consecuencias de desactivar la ejecución de estos procedimientos, cuando dicha opción esté disponible para el usuario. No obstante, el rechazo que generalmente produce este tratamiento, provoca que rara vez el interesado sea informado de su existencia.

Sólo resta indicar que, a mi entender, la modificación de la LSSI por parte de la Ley de Firma Electrónica (Ley 59/2003, de 19 de diciembre, Disposición Adicional 8ª) lo que ha venido es, en algunos casos a modificar (como en relación con el envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente) la competencia para la imposición de sanciones, pero en otros (como en el caso de las cookies) a clarificar una competencia que –a mi entender– siempre ha sido de la AEPD.

2. PRINCIPALES SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN CON INCIDENCIA EN LA PROTECCIÓN DE DATOS PERSONALES

Una vez analizada la conceptuación de determinados signos como datos de carácter personal, ya estamos en disposición de analizar los principales servicios de la sociedad de la información con incidencia en la protección de datos personales.

Los servicios que permite la Sociedad de la Información son diversos, así como el tratamiento de datos personales realizados como consecuencia de su desarrollo. A continuación analizamos, desde la óptica de la protección de datos, algunos de ellos.

2.1. Prestadores de Servicios de Intermediación

En primer lugar (por su evidente importancia en esta materia) nos referiremos a los "prestadores de servicios de Intermediación" (en adelante PSI), según la terminología acuñada por la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico, (en adelante, LSSI). Dentro de los PSI la LSSI distingue entre: Operadores de redes y proveedores de acceso; aquellos que realizan copia temporal de los datos solicitados por los usuarios; prestadores de servicios de alojamiento o almacenamiento de datos; y, por último, aquellos que facilitan enlaces o instrumentos de búsqueda.

2.1.1. Proveedores de acceso a Internet

Los proveedores de acceso a Internet son, como su propio nombre indica, empresas que permiten al usuario final acceder a la red. Proveedores son tanto

grandes plataformas (Telefónica, BT...), como otras empresas más pequeñas que se sitúan entre las primeras y el usuario final. Estas empresas compran líneas de gran capacidad a las grandes plataformas y las venden "a trocitos" a los usuarios finales. Normalmente, los Proveedores de acceso suelen ofrecer otros servicios al cliente, principalmente espacio para alojar su web y correos electrónicos, vinculados al dominio del proveedor o al del usuario (en el supuesto de que disponga de él), pero nos referimos aquí a su actividad estrictamente como proveedores de acceso.

Los proveedores de acceso almacenan y someten a tratamiento datos personales de los usuarios que han contratado sus servicios de acceso a Internet. Hay que ser consciente –como indica la AEPD en sus Recomendaciones para usuarios de Internet– cuando se suministran datos personales a un proveedor de acceso de a quién se facilitan y con qué finalidad. Y si esta máxima es aplicable siempre que comuniquemos nuestros datos a terceros, en el caso de la cesión de datos a los proveedores de acceso a Internet es especialmente importante. Ello es asi dado que suelen disponer de información, como la dirección IP de la máquina del usuario, que si bien no es *per se* un dato de carácter personal (según la opinión que hemos mantenido), la posibilidad de relacionarla con una persona determinada –que está a su alcance, por su propia condición de proveedores de acceso– la convierte en un poderoso instrumento de marketing.

Si el conocimiento y uso de la IP del cliente es razonable que se conozca por el proveedor de acceso para las tareas asociadas al servicio contratado también será lo cierto que, salvo que se solicite el consentimiento, no existe habilitación legal para que el mismo disponga de otros datos diferentes a esta, como puedan ser los datos de tráfico, al menos en tanto en cuanto no se desarrolle reglamentariamente la obligación de retención de datos de tráfico que contempla el artículo 12 de la LSSI.

2.1.2. Los buscadores

Otro servicio de intermediación que recoge la LSSI son "aquellos que facilitan enlaces o instrumentos de búsqueda" (que nosotros denominaremos "buscadores"). Un buscador es un sitio web cuya función principal consiste en proporcionar un medio para recolectar y proporcionar información acerca del contenido de otros sitios en Internet.

Lo cierto es que, cada día más, los buscadores se configuran como auténticas puertas de entrada a Internet, de donde se puede extraer ingente información sobre gustos y preferencias. Y si bien, en principio, los mismos no tratan de datos de carácter personal, la posibilidad de cruzar dicha información almacenada con datos personales convierte su actividad en potencialmente muy peligrosa para el usuario. No será extraño encontrar políticas de privacidad de buscadores

en las que se haga referencia a la recogida de "Información anónima"[15]. Esta información, en principo anónima y que se basa en la IP o dominio del usuario, se convierte automáticamente en dato de carácter personal al cruzarla con algún dato personal del usuario.

2.1.3. Prestadores de servicios de hosting y housing

Por último nos referiremos a los "prestadores de servicios de alojamiento o almacenamiento de datos" (servicios que "generalmente" se suelen conocer como "hosting" y "housing"). Hay diferentes criterios de distinción y variedades de estos servicios. Pero utilizaremos la denominación más simplificadora, según la cual: se entiende por housing el hospedaje del ordenador en las instalaciones del prestador del servicio y por hosting o webhosting el almacenamiento de unos datos y la prestación de unos servicios en un ordenador conectado a Internet permanentemente para que pueda accederse a ellos desde cualquier punto del mundo y a cualquier hora.

La principal vinculación de estos servicios (que denominaremos conjuntamente como hosting) con la protección de datos es que constituyen el supuesto paradigmático de tratamiento de datos por terceros en Internet[16]. Efectivamente, si el supuesto paradigmático de tratamiento de datos por terceros lo constituyen las asesorías –pues son el caso típico de encargado de tratamiento–, en Internet esta consideración podemos afirmarla respecto de estos prestadores.

---

15. Efectivamente, es habitual que los buscadores traten lo que –en terminología del buscador Altavista (www.altavista.com)– se denomina "información anónima" a lo que responden textos en la política de privacidad como el siguiente:

"Información anónima" no es "información personal identificadora". Información anónima es información sobre la forma en que usted utiliza nuestra página (paginas que usted visita y búsquedas que realiza). La información anónima también incluye el nombre de dominio y/o direcciones I.P. (según se explica abajo) de buscadores de Internet que visitan nuestra página, la hora del día en que se visitó la página y otra información no personal".

16. Como sabemos el "Encargado de Tratamiento" es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento (artículo 3.g de la LOPD). Nos encontramos ante la figura del encargado del tratamiento cuando los datos titularidad del responsable del fichero son tratados por un tercero ajeno a su organización. Como sabemos la justificación del tratamiento que ese tercero hace de los datos viene dada por el hecho de que el acceso a la información de carácter personal por el tercero es necesario para la prestación de un servicio al responsable, lo que justifica la existencia de un régimen jurídico específico que, entre otras cosas, se caracteriza por la "sustitución" de la exigencia de recabar el consentimiento del interesado para proceder a la cesión de los datos al tercero, por la firma de un contrato entre responsable del fichero y encargado del tratamiento que contenga –como mínimo- el contenido del artículo 12 LOPD. Es habitual la existencia de supuestos de tratamiento por terceros tanto en el "mundo analógico" como en el "mundo on line".

La consideración de los mismos como encargados de tratamiento –cuestión discutida por algunos autores– es confirmada por la AEPD en la memoria del año 2000, al establecer:

> dentro del concepto de servicios informáticos, existe una amplia gama de modalidades, que incluyen: colocación y almacenamiento de equipos (generalmente, propiedad de la organización que encarga los servicios), conexión de los equipos a Internet, asistencia técnica, colaboración en la resolución de averías y otras tareas de mantenimiento. Al conjunto de estos servicios se le suele denominar "housing". Cuando el servicio prestado supone exclusivamente la administración de los servidores se le denomina "hosting ". En ambos casos, aunque de diferente forma, el personal que presta los servicios suele tener acceso a los ficheros de la compañía, pues tanto para unas tareas como para las otras se requiere un perfil de usuario con privilegios generalmente reservados al administrador de la máquina, por lo que nos hallamos ante la figura del encargado de tratamiento.

También –continúa diciendo la AEPD–

> se han encontrado varios casos en los que los servicios de "hosting" o "housing" se prestan por compañías 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 en absoluto a la legislación española.

En ambos casos aunque de diferente forma –concluye–,

> el personal que presta los servicios suele tener acceso a los ficheros de la compañía, pues tanto para unas tareas como para otras se requiere un perfil de usuario con privilegios generalmente reservados al administrador de la maquina.

Aunque en su día mantuvimos que considerar estos servicios como supuestos de encargados de tratamiento en todo caso suponía un error pues –decíamos– que

> la práctica demuestra que, en ocasiones, la empresa que ofrece el servicio de alojamiento y mantenimiento informático no tiene acceso autorizado a los ficheros con datos de carácter personal de la compañía que ha encargado el servicio.

Lo cierto es que la lectura detenida del concepto de tratamiento de la LOPD evidencia que su excesiva laxitud (por tratamiento de datos hay que entender las "operaciones y procedimientos técnicos de carácter automatizado, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación...", artículo 3.c. de la LOPD)", permite englobar la actividad de hosting (siempre que se alogen datos de carácter personal en la sede del proveedor) como un supuesto de tratamiento de datos (pues al menos se produce una "conservación" de los mismos) que se efectúa por dicho tercero.

2.2. Otros prestadores de servicios de la sociedad de la información

Como hemos mencionado anteriormente, además de los PSI existen otros muchos prestadores de servicios de la sociedad de la información. En las próximas líneas analizaremos la incidencia de algunos de ellos en materia de protección de datos.

2.2.1. World Wide Web (www)

Uno de los principales servicios de Internet, junto con el correo electrónico, es la www. El principal problema que suele plantear la utilización de este servicio es la elaboración de perfiles de los usuarios que acceden al mismo. Las soluciones técnicas ofrecidas, tales como la utilización de servidores anónimos[17], no son ni conocidas ni cómodas para el usuario que, preocupado por la salvaguarda de su intimidad, puede decidir adoptarlas.

Si, como he sostenido anteriormente la IP puede constituir indirectamente un dato de carácter personal, por cuanto se puede relacionar con un dato que identifique a la persona, hemos de estar especialmente atentos a las políticas de privacidad de aquellas webs en las que comuniquemos información de carácter personal, tanto si ésta es simplemente nuestra dirección de correo electrónico, como si es el nombre y apellidos, dado que constituye una declaración formal de intenciones del titular del site, en la que manifiesta la naturaleza de los datos recabados en el mismo y la finalidad a la que van a ser destinados, de modo que el interesado conozca en todo momento el tratamiento que va a tener la información por él facilitada, ofreciéndosele la posibilidad de consentirlo.

2.2.2. Chatting (servicio de conversación electrónica, irc, o simplemente conocido como chat)

Según la definición de la AUI[18]

> se trata de un servicio que permite la conversación simultánea entre varios usuarios a través de la red. Funciona mediante la conexión a un servidor en el que se elegirá un grupo de conversación o canal. Cada participante se da a conocer a los demás a través de un seudónimo o nickname. Si el programa de conversación está preparado para ello, se pueden utilizar, además del intercambio escrito, servicios de conversación oral y videoconferencia.

17. Los servidores anónimos actúan como una especie de tiendas de máscaras que ofrecen al que entra en ellos una máscara o nueva identidad con la que el mismo podrá actuar sin ser identificado. Desgraciadamente su utilización, lejos de servir para proteger la intimidad, suele servir para enmascarar actividades ilícitas.

18. Se puede consultar en www.aui.es

Para analizar la incidencia de la protección de datos en el servicio de Chat habrá que tener en cuenta que en la mayor parte de los chats se permite al usuario la posibilidad de identificarse con un nickname o seudónimo. Pero existe la posibilidad real de que el usuario se identifique mediante sus datos personales. Parece lógico, pues, en la medida en que el proveedor del servicio de chat únicamente disponga de los seudónimos de los usuarios, que no sea necesario cumplir con lo dispuesto en la LOPD, al no encontrarnos con dato de carácter personal alguno. Sin embargo, cuando es posible relacionar ese nick con datos identificativos de la persona, sí estaríamos obligados al respeto y cumplimiento de la legislación sobre protección de datos. Entendemos que, en este último caso, el criterio aplicable es similar al adoptado en el supuesto del correo electrónico, ya analizado.

Aunque en la mayor parte de los chats existentes hoy en día no se solicita ningún dato de carácter personal para poder participar en los mismos, existen otros en los que la inscripción se produce a través de la cumplimentación de un formulario y la remisión de la clave de acceso por correo electrónico. En estos casos, el acceso al servicio conlleva, ineludiblemente, el tratamiento, por el responsable del chat, de información de carácter personal de los usuarios. Pese a ello, pocos son los portales que ofrecen servicios de chat y disponen de política de privacidad, impidiendo así al usuario conocer el destino y finalidad del tratamiento de sus datos. Además, aquellos portales que sí publican una política de privacidad, no suelen referirse expresamente al tratamiento de datos en este tipo de servicios, incidiendo mucho más en otro tipo de aspectos.

2.3. El tercero de confianza

A los efectos de ofrecer mayores garantías a la hora de contratar un servicio o un bien por Internet, la LSSI crea (en su artículo 25) la figura del Tercero de Confianza. Este podrá ser utilizado por las partes de un contrato para archivar en soporte informático las declaraciones de voluntad que integran los contratos electrónicos y consignar la fecha y la hora en que dichas comunicaciones han tenido lugar, siendo admisible en juicio, como prueba documental, el documento electrónico en donde se archiven tales contratos. En este sentido la Ley, al referirse a las obligaciones del prestador de servicios frente al consumidor, previas al inicio del procedimiento de contratación, exige al primero el deber de informar al consumidor de si "va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible (artículo 27.1.b. LSSI)".

Con el recurso a tales Terceros de Confianza se podrá constatar cuáles fueron los términos del contrato alcanzado entre las partes, siendo admisible en juicio el documento electrónico en donde se habrá archivado tal contrato[19].

19. Para un análisis más detallado de los aspectos que la incorporación al proceso de tales soportes informáticos supone véase: "La prueba por medios audiovisuales e instrumentos de archivo en la Lec 1/2000". Sanchis Crespo C. y Chaveli Dont, E. Valencia: Tirant lo Blanch, 2002.

El funcionamiento de esta institución se puede articular –al menos– de dos formas: el tercero de confianza vía web y el tercero de confianza vía email. En el primero de los supuestos el tercero de confianza archiva el contrato que se formaliza cuando un usuario realiza una transacción en una web; por el contrario, en el segundo de los supuestos el tercero de confianza archiva los correos electrónicos que se intercambian las partes. Ambas modalidades, aunque en el fondo responden a una misma institución y por lo tanto las consideraciones jurídicas que realizaré son válidas para ambas, suponen peculiaridades en la forma de cumplir las obligaciones.

Por lo que respecta al posicionamiento jurídico que en materia de protección de datos tiene esta figura he de decir que aunque se trata de un supuesto que *prima facie* pueda parecer un claro ejemplo de tratamiento de datos por terceros (pues indudablemente existe un tercero que, para prestar el servicio, accede a datos de las partes) no es menos cierto que la existencia de una obligación de mantener los datos por un periodo determinado (en este caso de 5 años) nos lleva a considerar que tal supuesto "choca" con la obligación impuesta al encargado del tratamiento por el artículo 12 LOPD de destruir o devolver tales datos al responsable del fichero. Tampoco han tenido mucho éxito las interpretaciones tendentes a dar cobertura a esa legitimación de mantenimiento de los datos después de acabado el contrato (y por tanto sin necesidad de destruirlos o devolverlos) acudiendo al artículo 16 de la LOPD, pues la AEPD entiende que el mismo es aplicable (normalmente) sólo al responsable del fichero, y no al encargado del tratamiento.

Por ello entendemos que habría que poner en relación dicho servicio con el supuesto de cesión necesaria del artículo 11.2.c que dispone que no será necesario el consentimiento:

> Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

Lo que a su vez habría que poner en relación con la exención del deber de información del artículo 27.2:

> La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por Ley.

Como sabemos el "apartado anterior" dispone:

> 1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

Aunque esta interpretación es, a mi juicio, la correcta, es arriesgada pues parte de considerar que existe una exención del deber de recabar el consentimiento y de cumplir con el deber de información. Por ello no estará de más, en tanto en cuanto lo permita la lógica vertebración del servicio recabar el consentimiento (siquiera sea tácito) y cumplir con el deber de información.

3. TRANSFERENCIA INTERNACIONAL DE DATOS (TID)

3.1. Concepto

Se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. 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. Norma Primera, Instrucción 1/2000, relativa a las normas por las que se rigen los movimientos internacionales de datos.

Podría plantearse, y así ha ocurrido, que en el caso de Internet y debido al carácter extrateritorial que implícitamente tiene este medio, la simple publicación de datos en Internet supone una trasferencia Internacional de Datos.

En la Sentencia de 6 de noviembre de 2003 (asunto C-101/01)[20] el Tribunal de Justicia de la Unión Europea concluye:

> los datos personales que llegan al ordenador de una persona que se encuentra en un país tercero y que proceden de una persona que los ha publicado en un sitio Internet, no han sido objeto de una transferencia directa entre estas dos personas, sino que se han transmitido con la ayuda de la infraestructura informática del proveedor de servicios de alojamiento de páginas web donde está almacenada la página.

20. Además de su trabajo retribuido como empleada de mantenimiento, la Sra. Lindqvist desempeñaba funciones de catequista en la parroquia de Alseda (Suecia). Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página web en Internet. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran. A petición suya, el administrador del sitio Internet de la Iglesia de Suecia creó un enlace entre las citadas páginas y dicho sitio. Las páginas web de que se trata contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, sólo su nombre de pila. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Asimismo, señaló que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad. La Sra. Lindqvist no había informado a sus compañeros de la existencia de estas páginas web, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion (organismo público para la protección de los datos transmitidos por vía informática). En cuanto supo que algunos de sus compañeros no apreciaban las páginas web controvertidas, las suprimió.

Ya que, en dicho caso

> no contenían los mecanismos técnicos que permiten el envío automático de la información a personas que no hayan buscado deliberadamente acceder a dichas páginas.

Es decir, parece que del texto trascrito se puede concluir que: en Internet hay trasferencia Internacional de Datos cuando se hace llegar la información a alguien que, sin buscarla deliberadamente, y estando en otro país, le llega, pero que la simple publicación en Internet no constituye trasferencia Internacional de datos.

Cosa diferente es (obviamente) el hecho de que la mera publicación de datos en Internet supone, como se encarga de aclarar la misma sentencia un tratamiento automatizado de datos y una cesión de los mismos[21].

Una vez aclarado el concepto de Trasferencia Internacional de Datos y concretado en Internet, vamos a analizar su régimen jurídico.

3.2. Régimen Jurídico

La regla general, establecida en el artículo 33 de la LOPD, parte de la imposibilidad de realizar cualquier TID, ya sea temporal o definitiva, con destino a países que no proporcionen un nivel de protección equiparable al que presta la LOPD, sin contar con la autorización previa del Director de la Agencia de Protección de Datos.

No obstante, esta autorización no es necesaria cuando la misma trae causa de las excepciones establecidas en el artículo 34 de la Ley, en las que se basan algunas de las TID más frecuentes que se producen en Internet:

1.- 34.f. "Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero". Un ejemplo de esta excepción, aplicado a Internet lo constituye el caso en que haya que realizar una adquisición on line en una página web ubicada en el extranjero y se deban facilitar a la misma dichos datos personales necesarios para la perfección de la operación –número de cuenta corriente o tarjeta, domicilio, etc.–.

2.- 34.e. "Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista". Se trata ésta de una hipótesis muy común, en la que el

21. En este sentido, dice la citada Sentencia: "La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46."

Responsable del Tratamiento, a través de la política de privacidad publicada en su página web, recaba el consentimiento expreso del interesado para la TID de la que está siendo informado.

3.- 34.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". Este supuesto se produce cuando solicitamos la entrega del producto adquirido vía web a un tercero que se halla en el extranjero. La compañía vendedora (responsable del fichero) suscribe un contrato con el comprador, que lo adquiere para el interesado, de quien necesariamente debe facilitar los datos para que pueda efectuarse la entrega. Al estar en el extranjero, necesariamente deberán transmitirse estos datos a la empresa logística encargada de hacer llegar el producto a su destinatario.