Protección de datos de carácter personal en la Administración Electrónica

(Protection of personal data in e-Government)

Bacaria Martrus, Jordi
Eusko Ikaskuntza. Miramar Jauregia. Miraconcha, 48.
20007 Donostia – San Sebastián

BIBLID [1138-8552 (2008), 20; 61-82]
Recep.: 27.05.04
Acep.: 17.10.08

El uso de sitios webs en el sector público y el establecimiento de relaciones por vía electrónica con los ciudadanos conlleva nuevos tratamientos de sus datos y requiere la actualización normativa sobre intimidad y protección de datos para que las administraciones públicas cumplan su imperativo legal y especialmente para generar confianza en los ciudadanos.

Palabras Clave: Protección de datos de carácter personal en Internet. Administración electrónica. LSSI. Websites. Comunicaciones comerciales por vía electrónica.

Sektore publikoan web guneak erabiltzeak eta hiritarrekin harremanetan jartzeko sare elektronikora jo izanak, datu pertsonalak beste modu batean kudeatzearen beharra eragin ez ezik intimitatearen eta datuen babeserako neurriak eguneratzearen beharra azaldu du, administrazio publikoek beren betebehar legalak bete ditzaten eta, batez ere, hiritarren artean konfiantza sustatzeko.

Giltza-Hitzak: Izaera pertsonaleko datuen babesa Interneten. Administrazio elektronikoa. Informazio Gizartearen Zerbitzuen Legea. Web guneak. Sare elektronikoaren bidezko komunikazio komertzialak.

L'utilisation de sites web dans le secteur public et l'établissement de relations avec les citoyens via Internet implique de nouvelles formes de traitement des données et exige une actualisation normative en matière d'intimité et de protection des données, afin que les administrations publiques respectent les lois en vigueur et comptent sur la confiance des citoyens.

Mots Clé : Protection des données personnelles sur Internet. Administration électronique. LSSI. Sites web. Communications commerciales via courrier électronique.

1. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN INTERNET

1.1. El derecho a la Protección de Datos en la nueva Constitución Europea

En el inicio de este trabajo dedicado, en general, a la protección de datos personales en Internet y específicamente al tratamiento de datos de carácter personal por la que hemos llamado Administración electrónica, es oportuno citar que el texto actual del proyecto de la futura Constitución Europea, dentro de la Carta de los Derechos fundamentales de la Unión, establece en su artículo II-8 relativo a la Protección de Datos de Carácter Personal que "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen".

La formulación de este principio con tanta claridad conceptual sitúa el derecho a la protección de datos en el núcleo de los derechos de la persona física o incluso jurídica, sin distinción del dato ni de su tratamiento automatizado o manual o en sede electrónica, y ya no centrado en cualquier otro significado complementario relativo a la intimidad, privacidad u honor de la persona.

1.2. La aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal al tratamiento de datos personales en Internet

De acuerdo con su artículo 1, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal tiene por objeto

> garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El propio artículo 3 de la Ley Orgánica define el Tratamiento de datos personales como

> operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Aunque no hay ningún tipo de duda sobre que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal es una disposición aplicable a la red Internet, sí es cierto que desde la publicación y entrada en vigor de la mencionada ley ha aumentado de manera espectacular el uso de Internet a todos los niveles y especialmente por lo que se refiere a los negocios digitales, al comercio electrónico, en general, a los servicios de la sociedad de la información.

Asistimos, asimismo, a un auge imparable de las relaciones de la Administración con los ciudadanos por medios electrónicos.

La propia Agencia de Protección de Datos dictó en el año 2000 unas recomendaciones 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.

A partir de una inspección sectorial en el año 2000, cuyo objetivo era determinar si las entidades que actualmente desarrollan su actividad comercial a través de Internet cumplían con los principios de la legislación vigente en materia de protección de datos, la Agencia Española de Protección de Datos estableció unas Recomendaciones para el cumplimiento de la LOPD en Internet, referidas a la información en la recogida de datos, el consentimiento del afectado, los usos y finalidades del dato, la cancelación de los datos, el tratamiento de datos de salud y de vida sexual, la regulación del acceso a los datos por cuenta de terceros, la comunicación de datos, el movimiento internacional de datos y la seguridad de los datos.

1.3. El derecho fundamental a la protección de datos en la doctrina del Tribunal Constitucional

La Sentencia del Tribunal Constitucional de 30 de noviembre del 2000 concibe el Derecho a la Protección de Datos como un derecho fundamental que persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y su destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del titular de los datos.

Según el alto Tribunal, el objeto de protección no se limita solamente a los datos íntimos de la persona, sino a cualquier clase de datos personales, sean o no íntimos, cuyo conocimiento o utilización por terceros pueda afectar a sus derechos, sean o no fundamentales y, por tanto, alcanza a las relaciones jurídico administrativas "on line" o por vía electrónica.

La Protección de estos datos, entendido como un derecho fundamental, alcanza aún mayor importancia en un medio como Internet en el que los datos de carácter personal pueden circular y transmitirse, gracias a la tecnología, con mayor facilidad fuera del control de su titular.

En el tratamiento de datos de carácter personales en la red Internet, permanece, por tanto vigente, el objetivo fundamental del Derecho a la Protección de Datos de garantizar a una persona un poder de control sobre sus datos personales como usuaria de Internet.

1.4. La Sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003, asunto Lindqvist

La Sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003 sobre el ámbito de aplicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las

personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos, sobre el asunto Lindqvist, resolvió que

> la conducta que consiste en hacer referencia, en una página web, a varias 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 afecciones, constituye un tratamiento total o parcialmente automatizado de datos personales en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 d'octubre de 1995, relativa a la protección de las personas físicas en aquello que se refiera al tratamiento de datos personales y a la libre circulación de estos datos.

El Tribunal de la Unión fundamenta su tesis en que el concepto de tratamiento de datos que establece el artículo 3, apartado 1, de la Directiva 95/46, comprende: "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales", citando ejemplos de tales operaciones enumerados en el mencionado precepto, entre los que figuran la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos.

Por todo ello, queda avalada por esta sentencia Europea la aplicación a la red Internet de la legislación sobre protección de datos de carácter personal.

1.5. El rastro de Datos Personales en Internet

Las posibilidades de dejar rastro en la red de los datos identificativos de la persona e incluso de datos económicos o de datos personales relativos al perfil del individuo por parte de los usuarios de Internet, durante el acceso a páginas web, en las transacciones de comercio electrónico o bien cuando se utiliza el correo electrónico, que den como resultado una pérdida del poder de control del titular de los datos pueden ser numerosas:

– La dirección IP ("Internet Protocol"), que consiste en una dirección física, con un número único e irrepetible de identificación asignado a cada Ordenador Personal dentro de Internet que será conocida en el momento que realicemos en Internet cualquier tipo de operación.

– Las "cookies" actúan como bloques de datos que algunos sitios web envían a nuestro Ordenador Personal cuando accedemos a ellos. En cada ocasión que accedemos a ese sitio Web, nuestro PC reenviará esa "cookie" al sitio web. Una "cookie" podría llegar a contener datos como "passwords", "logins" o datos de identificación o datos para una compra.

No es imposible que las "cookies" puedan constituir un elemento o un medio para la obtención de datos de carácter personal que identifiquen o puedan identificar al individuo en sus conexiones en Internet. Sería el caso de contenidos de "cookies" de un web que asocian los datos con el usuario, permitiendo adicionar

datos complementarios para la elaboración de un perfil que podría llegar a ser muy sensible.

También hay "cookies" que funcionan como un método de autenticación de usuario, permitiendo 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 requerirse su contraseña como medio para autenticar su identidad.

"Mailing lists", Grupos de noticias, "Chatting" o conversación electrónica, que son sistemas o canales de intercambio de información o foros de debate mediante correo electrónico u otros datos identificativos del titular.

Los datos personales de los usuarios de los mencionados servicios u operaciones o simplemente de quienes acceden a los sitios Web del sector privado o del sector público, y específicamente sus datos de correos electrónicos y sus datos de tráfico pueden ser recolectados por medio de almacenamientos invisibles de datos, enlaces invisibles a otros sitios web o pueden seguir rutas desconocidas, circulando o siendo transferidos a un país que no disponga de garantías legales equivalentes sobre protección de datos.

Además, en el caso de las comunicaciones por medio de correos electrónicos, los datos personales de los emisores de los correos pueden ser recogidos, tratados, cedidos o utilizados para el envío de las comunicaciones electrónicas de modo ilegítimo y al margen de la legalidad establecida en la LOPD o en la LSSI.

1.6. La consideración de Internet como una fuente no accesible al público

Parece que no ofrece ningún tipo de duda que la red Internet no puede ser considerada una fuente accesible al público, a los efectos de tratamiento de datos personales sin consentimiento del interesado.

El fundamento que se ha dado a esta afirmación es por un lado de carácter técnico: Internet no es propiamente una fuente que contenga datos personales, sino que es solamente un soporte de la información.

Por otra parte, existe un argumento legal que es inapelable: el artículo 3. j) de la LOPD no incluye Internet en su listado limitativo de fuentes accesibles al público.

En la medida que Internet no sea una fuente accesible al público, los datos de carácter personal incluidos en las páginas web no podrán tratarse sin consentimiento del interesado, a no ser que se encuentren en publicaciones electrónicas equivalentes a las fuentes que establece el artículo 3. j) de la LOPD: listas de grupos profesionales, diarios y boletines oficiales, medios de comunicación, repertorios telefónicos y el censo promocional.

De este modo, los datos personales que puedan encontrarse en Internet deberán ser tratados en todo caso de acuerdo con la finalidad del dato.

No obstante, a mi modo de ver, no siempre resulta fácil determinar claramente la finalidad del dato difundido en Internet por el propio titular, y no deberíamos descartar que sobre ciertos datos personales comunicados en la red habría la posibilidad de aplicar el consentimiento tácito del interesado que difunde sus dato en Internet cuando no se pueda determinar claramente la finalidad del dato.

2. ASPECTOS DE PROTECCIÓN DE DATOS EN LA LEY 34/2002, DE 30 DE JULIO, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO: SU APLICACIÓN A LA ADMINISTRACIÓN PÚBLICA

2.1. La aplicación de la Ley 34/2002, de 30 de julio, de servicios de la sociedad de la información a las Administraciones públicas

La Ley 34/2002, de 30 de julio, de servicios de la sociedad de la información y de comercio electrónico es de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario y también a servicios no remunerados, en la medida en que constituyan una actividad económica para el prestador de servicios.

Tiene interés detenernos en algunas definiciones de la LSSI a fin de delimitar su posible aplicación a las administraciones públicas.

En la definición de servicio de la sociedad de la información, la LSSI incluye también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios entre los que cita el suministro de información por vía telemática y el envío de comunicaciones comerciales por vía electrónica.

Asimismo, son también servicios de la sociedad de la información, de acuerdo con la LSSI, los servicio de intermediación por los que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Por otra parte, nos interesa analizar la definición de la ley sobre comunicaciones comerciales:

> Toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

En cambio, de acuerdo con la LSSI, no constituirán servicios de la sociedad de la información el intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

De las definiciones anteriores podemos afirmar sin ninguna duda que las actividades de las administraciones públicas no quedan excluidas como norma general de la aplicación de la Ley 34/2002, de 30 de julio, de servicios de la sociedad de la información y de comercio electrónico, si entendemos que aquellas realizan normalmente actividades económicas. Los mencionados preceptos se refieren a la aplicación de la LSSI a servicios de la sociedad de la información de los que las administraciones públicas pueden ser titulares: servicios de acceso a la información o de información por vía telemática, de utilización indirecta de otros servicios de la sociedad de la información o el acceso a la información o comunicaciones por vía electrónica relativas a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de un órgano de la administración.

En todo caso, aunque las actividades de las Administraciones públicas en el estricto ejercicio de sus funciones de servicio público podrían tener un difícil encaje en la aplicación general de la Ley de servicios de la sociedad de la información y de comercio electrónico, se deberá tener en cuenta, no obstante, por un lado las posibilidades abiertas en el análisis anterior de las definiciones de la LSSI, especialmente cuando las administraciones públicas lleven a cabo actividades sujetas al derecho privado; por otra parte entiendo que la Ley 34/2002, de 30 de julio, de servicios de la sociedad de la información y de comercio electrónico debería aplicarse en todo caso con carácter residual en aras a la seguridad y coherencia en la aplicación del derecho.

Finalmente, será necesario atender, con carácter general, también por parte de las administraciones públicas, las normas sobre Protección de Datos contenidas en la Ley 34/2002, dependiendo de su posición como sujeto de las distintas relaciones jurídico administrativas.

2.2. Las remisiones de la Ley 34/2002 a la normativa sobre protección de datos

Las remisiones de la Ley de servicios de la sociedad de la información y de comercio electrónico a la aplicación de la legislación sobre protección de datos de carácter personal y en general al derecho a la protección de datos, se refieren a las relaciones jurídicas que nacen de las comunicaciones electrónicas o de los contratos celebrados por medios electrónicos o de los propios servicios de intermediación en Internet y, a la vez, a las actuaciones o procedimientos de la administración de carácter sancionador o de simple tutela administrativa que la Ley 34/2002 regula.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico establece en su artículo primero, dedicado al objeto de la ley, que "las disposiciones contenidas en esta ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas... o que tengan como finalidad... la protección de datos personales".

Este precepto de la Ley 34/2002 realiza una remisión externa expresa a nuestra legislación sobre Protección de Datos, entendiendo dicha legislación en el plano normativo comunitario, estatal y autonómico e integrando la nueva norma en nuestro sistema jurídico, con el objetivo de reconocer y respetar el derecho fundamental de la protección de datos, definido por la Sentencia del Tribunal Constitucional 292/2000 y anclado en el artículo 18 de nuestra Constitución.

En realidad, ya no cabía duda, como ya se ha comentado en el apartado primero de este trabajo, sobre la aplicación de Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal al tratamiento de datos personales en los negocios jurídicos por vía electrónica y a la comunicación y transmisión de información a través de redes de telecomunicaciones. Ello se desprende claramente del ámbito de aplicación de la Ley 15/1999, de las definiciones de datos y tratamiento de datos de su artículo 3, de lo dispuesto en el propio Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, aprobado por el Real Decreto 994/1999de 11 de junio y del desarrollo de la Ley 15/1999 por parte de la Agencia de Protección de Datos en sus Recomendaciones sobre Internet y el Comercio Electrónico.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico realiza otras remisiones a la Protección de Datos, referidas a actuaciones sancionadoras de la administración o a obligaciones de proveedores de servicios o de operadores de redes en relación a las actuaciones sancionadoras mencionadas entre las que cabe destacar especialmente, entre otras, la regulación del deber de retención de datos del artículo 12 de la LSSI.

Textos de las remisiones a la Protección de Datos citada en la Ley 34/2002	Artículos de la LSSI en las que se citan las remisiones
"las disposiciones contenidas en esta ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas... o que tengan como finalidad... la protección de datos personales"	**Artículo 1.1 de la LSSI** ***Objeto de la Ley***
"en la adopción y cumplimiento de las medidas (restrictivas)", establecidas en el citado artículo 8, "se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos... a la protección de los datos personales"	**Artículo 8 de la LSSI** ***Restricción a la prestación de servicios***
"Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios... deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración (de los datos) y el acceso no autorizado a los mismos" "La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales"	**Artículo 12 de la LSSI** ***Deber de colaboración de los prestadores de servicios de intermediación***
"... será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo"	**Artículo 19 de la LSSI** ***Comunicaciones comerciales electrónicas***
"Si el destinatario de servicios debiera facilitar su dirección de correo electrónico durante el proceso de contratación o de suscripción a algún servicio y el prestador pretendiera utilizarla posteriormente para el envío de comunicaciones comerciales, deberá poner en conocimiento de su cliente esa intención y solicitar su consentimiento para la recepción de dichas comunicaciones, antes de finalizar el procedimiento de contratación"	**Artículo 22 de la LSSICE** ***Contratos celebrados por vía electrónica***

* Cuadro incluido en la publicación "Las claves para la Gestión de Datos Personales en los Negocios Electrónicos", © Jordi Bacaria – Ediciones Experiencia.

2.3. La obligación de información del artículo 10 de la Ley 34/2002: su aplicación a la administración electrónica

El artículo 10 de la Ley 34/2002 obliga a los prestadores de servicios de la sociedad de la información a disponer de los medios que permitan a los destinatarios del servicio y a los órganos competentes, acceder por medios electrónicos a cierta información, que en el caso de personas físicas, constituye una información referida a la identidad de la persona y, por tanto, dato de carácter personal.

Estos datos no podrán utilizarse con otra finalidad distinta que la que se deduce de la obligación de información de la LSSICE, no pudiéndose considerar procedentes de fuente de acceso público en los términos del artículo 3.j) de la LOPD.

Por lo que se refiere a las personas jurídicas, éstas están obligadas a facilitar la siguiente información:

a) Nombre o denominación social.

b) Domicilio o dirección de uno de los establecimientos de la persona jurídica permanentes en España.

c) Dirección de correo electrónico y otros datos que permitan una comunicación directa y efectiva con la persona jurídica.

d) Los datos de la inscripción del nombre de dominio en un Registro Público.

e) Datos de autorización administrativa y del órgano habilitante, si procediera.

Las administraciones públicas no pueden estar exentas del cumplimiento de lo que dispone el artículo 10 de la Ley 34/2002 en aquello que fuera posible su aplicación y, no solo en aquellos supuestos en los que la administración actúa en régimen de derecho privado, por ejemplo a través de sociedades mercantiles, sino también con carácter general.

Entiendo que no cabe interpretar una excepción de las obligaciones del artículo 10 a favor de las administraciones públicas ya que la adaptación a la administración de la información exigida en el precepto, consistiría en el nombre del órgano o ente administrativo, su disposición de creación, domicilio, dirección postal o electrónica con fines de comunicación, y no se alcanzaría a entender el porqué de la no disponibilidad de esta información precisamente de las administraciones públicas, sometidas al régimen de transparencia administrativa.

2.4. El deber de retención de datos de tráfico relativos a las comunicaciones electrónicas del artículo 12 de la LSSI

Este precepto establece la retención de datos de conexión y tráfico generados por la prestación de un servicio de la sociedad de la información durante un periodo máximo de 12 meses. Los obligados por este precepto son:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones, que deberán conservar los datos relativos a la localización del equipo terminal empleado por el usuario.

b) Los prestadores de servicios de alojamiento de datos, que deberán conservar los datos relativos al origen de los datos y al momento en que se inició la prestación del servicio.

Los destinatarios finales de estos datos, según el apartado 3 del artículo 12, son los jueces, tribunales o el Ministerio Fiscal si los requieren en el marco de una investigación criminal o para la salvaguarda de la seguridad pública y la defensa nacional, así como las Fuerzas y Cuerpos de Seguridad.

a) Aplicación de la normativa sobre el secreto de las comunicaciones.

El artículo 12 establece el mantenimiento del secreto de las comunicaciones durante los procedimientos y operaciones de retención de datos. Hay que tener en cuenta que la aplicación de este precepto supondría la necesidad de un mandamiento judicial para la comunicación de los datos retenidos a las Fuerzas y Cuerpos de Seguridad, aunque permitiría su comunicación a los Jueces y Tribunales y a requerimiento del Ministerio Fiscal, de acuerdo con el artículo 18.3 de la Constitución española que garantiza el secreto de las comunicaciones.

b) Garantías sobre Protección de Datos.

El artículo 12 prevé, además de la referencia al mantenimiento del secreto de las comunicaciones, algunas garantías en relación a la Protección de Datos:

1. Finalidad del dato: el precepto prohíbe que los prestadores de servicios y los operadores de redes y servicios de comunicaciones electrónicas utilicen los datos retenidos para otros fines distintos del marco de investigaciones criminales, y de la salvaguardia de la seguridad pública y defensa nacional.

2. Comunicación de datos a las Fuerzas y Cuerpos de Seguridad: se hará respetando la normativa de datos personales y debemos añadir, como se ha hecho mención en el apartado anterior, respetando el secreto de las comunicaciones, es decir, por medio de mandamiento judicial.

3. Seguridad de los datos: se deberán adoptar las medidas de seguridad requeridas. Aquí se podría apuntar la posibilidad de que las medidas de seguridad necesarias para los ficheros con datos retenidos sean de nivel medio, en la medida que el conjunto de datos de carácter personal que puedan contener estos ficheros sean suficientes para permitir una evaluación de la personalidad de los usuarios del tráfico.

4. Clase de los datos con obligación de retener, el texto del artículo incluye dos especificaciones:

– Los datos con obligación de retener serán únicamente necesarios para la localización del equipo terminal empleado por el usuario para la transmisión de la información, o aquellos relativos a su origen y al momento en que se inició la prestación del servicio.

– Las categorías de datos que deberán conservarse se determinarán reglamentariamente, no pudiéndose entender esta previsión de otro modo que el desarrollo reglamentario no podrá ir más allá de precisar o concretar el tipo de datos que se deberán conservar por parte de los obligados a ello en el marco de lo que establece este mismo artículo 12: los datos necesarios para la localización del equipo terminal o los necesarios para conocer el origen de los datos y el momento en que se inició la prestación del servicio.

En cuanto a la duración del periodo de retención de los datos, el antiguo Ministerio de Ciencia y Tecnología ya ha avanzó que el Reglamento no agotará el plazo de la ley, tesis que sigue manteniendo el actualmente competente Ministerio de Industria.

c) Los datos retenidos como datos de carácter personal.

El primer interrogante que nos plantea el texto del artículo 12 es si los datos que se deben retener y conservar son datos de carácter personal, aunque su regulación parece que así lo prevé.

En caso que, efectivamente, se tratara de datos de carácter personal, la aplicación de este precepto supone la creación de un fichero automatizado con datos de carácter personal a fin de tratar estos datos, de los que serían titulares usuarios de Internet o consumidores por vía electrónica, por parte de los operadores de redes y servicios de comunicaciones electrónicas, de los proveedores de acceso a redes de telecomunicaciones y de los prestadores de servicios de alojamiento de datos, sin consentimiento del interesado.

El dato principal que los intermediarios de la sociedad de la información tienen posibilidad de retener es la dirección IP (Internet Protocol). La dirección IP consiste en una dirección fisica, con un número único e irrepetible de identificación asignado a cada Ordenador Personal en su conexión a la red Internet.

Será preciso, por tanto, determinar en primer lugar si la dirección IP, es o puede ser un dato de carácter personal, de acuerdo con la definición del artículo 3 de la Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal: “cualquier información concerniente a personas físicas identificadas o identificables”.

En todo caso, la cuestión esencial no consiste tanto en determinar si la dirección IP es un dato de carácter personal sino que se trata de definir si el objetivo de la retención de datos del artículo 12 persigue y haría posible una potencial identificación de la persona, por ejemplo, por medio de relacionar la dirección IP

de un PC con el correo electrónico del usuario, ya que el correo electrónico transmite la dirección IP; este supuesto encajaría en la definición de dato de carácter personal del artículo 3 de la Ley O. 15/1999.

d) La obligación de retención de datos en el marco de la Ley Orgánica 15/1999.

El supuesto de la obligación de retención de datos sin el consentimiento del titular del artículo 12 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico tiene su encaje normativo en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

Los preceptos aplicables de la Ley Orgánica 15/1999 al supuesto del artículo 12 son los artículos 6 y 11 en cuanto prevén excepciones al consentimiento sobre la recogida, tratamiento y cesión de datos. Por una parte, el artículo 6.1 de la Ley 15/1999 establece efectivamente que "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa" y por otra parte, el artículo 11.2.a) permite la cesión sin consentimiento del titular cuando esté autorizada por ley y el artículo 11.2.c) establece su cesión a Jueces, tribunales y Ministerio Fiscal.

El artículo 12 de la Ley 34/2002 recoge, no solo la obligación de recogida y tratamiento de datos de usuarios y consumidores de servicios de la sociedad de la información, sino que también establece la clase de datos y su finalidad, y también los supuestos específicos de comunicación de estos datos.

En este sentido, se entenderá que el Responsable del fichero deberá respetar y aplicar los derechos de información, acceso, rectificación y cancelación.

No parece que sea posible aceptar que, aún existiendo una previsión legal de recogida y tratamiento de datos sin consentimiento del interesado así como de comunicación de estos datos en supuestos específicos igualmente sin consentimiento, decaigan los derechos de información, acceso, rectificación y oposición. Aunque bien es cierto que los derechos de rectificación y de oposición estarían condicionados por la finalidad legal del fichero que recoja los datos retenidos, y en cuanto al derecho de cancelación, deberá atenderse al plazo máximo legal o al plazo reglamentario que se establezca de conservación de estos datos.

e) Consecuencias legales de la obligación de retención de datos.

En la medida que los datos retenidos puedan ser datos de carácter personal, la obligación de retención de datos conllevará un conjunto de consecuencias legales en el ámbito de la Ley Orgánica 15/1999 que afectarán a los operadores de redes y servicios de comunicaciones electrónicas, a los proveedores de acce-

so a redes de telecomunicaciones y a los prestadores de servicios de alojamiento de datos:

a. Creación de ficheros con los datos de tráfico y conexión de los usuarios.

b. Inscripción de los ficheros en el Registro General de Protección de Datos.

c. Aplicación de los derechos de información, acceso, rectificación y cancelación.

d. Cumplimiento de los principios generales de protección de datos.

En definitiva, por disposición legal, los prestadores de servicios de intermediación de la sociedad de la información, sin dejar de ser en los casos que así sea, encargados del tratamiento por el hecho de tratar datos de carácter personal por cuenta de terceros por la prestación de servicios de hosting y housing, pasarán a ser responsables de estos ficheros de datos retenidos.

2.5. Implicaciones del cumplimiento del artículo 12 para las administraciones públicas

La obligatoriedad del cumplimiento de los requerimientos del artículo 12 de la LOPD dependerá de la posición jurídica de las administraciones públicas en cada supuesto de hecho.

Será necesario tener en cuenta que aquellos órganos de la administración que asuman actuaciones como prestador de servicios o que participen en personas jurídicas cuya actividad sea la de actuar como prestadores de servicios, estarán sometidos al cumplimiento del artículo 12 de la LSSICE.

3. CUESTIONES SOBRE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN ELECTRÓNICA

3.1. Las relaciones con los ciudadanos a través de sitios Web de las administraciones públicas

Los sitios Web de numerosos órganos de la administración central y autonómica y especialmente de la administración local disponen de buzones electrónicos de consultas o de servicios electrónicos de información a fin de que los ciudadanos puedan remitir sus sugerencias o solicitudes de información a las administraciones públicas o puedan realizar gestiones o trámites administrativos por vía electrónica.

Por otra parte, algunas administraciones, especialmente ayuntamientos facilitan correos electrónicos gratuitos a todos los ciudadanos empadronados en los municipios respectivos.

3.2. Tipología actual de cuestiones sobre la aplicación de la LOPD a la Administración electrónica

a) Cuestiones referidas a leyendas de recogida y tratamiento de datos.

Se observa en webs de las administraciones la inexistencia de leyendas o cláusulas de recogida de datos.

También se observan leyendas o cláusulas de recogida de datos que confunden tratamiento de datos con cesión de datos, es decir bajo la fórmula de recogida de datos personales para su tratamiento por la administración, incluyen cesiones de datos, que podríamos llamar ocultas, a otras administraciones.

b) Cuestiones referidas a la finalidad del dato.

Algunas cláusulas o leyendas de recogida de datos personales en formularios electrónicos son incompletas y especialmente no incluyen la especificación de la finalidad del dato.

Esta cuestión tiene una relevancia legal muy importante para distinguir si la recogida de datos se hace con una finalidad de la Administración sometida a derecho público o al régimen del derecho privado.

c) Cuestiones referidas a cesión o acceso a los datos personales.

En muchas webs, mediante las cuales se recogen datos personales, existe confusión sobre la posición jurídica real de la administración titular del web, de la administración o administraciones titular o titulares del fichero, de la sociedad mercantil con capital público que gestiona el web, de los órganos de la administración que prestarán servicios o ante los cuales se podrán realizar gestiones por vía electrónica y entre quién ostenta la calidad de Responsable del Tratamiento o de Encargado de Tratamiento.

3.3. Aspectos del cumplimiento de la LOPD

Las actuaciones de la Administración por vía electrónica y las cuestiones generadas en el apartado anterior plantean las siguientes cuestiones específicas en relación al cumplimiento de la normativa sobre Protección de Datos:

a) Determinación del Responsable del Fichero y del Encargado del Tratamiento en los casos de intervención de un prestador de servicios externo a la Administración.

Particularmente en los casos de la intervención de un prestador de servicios con la finalidad de facilitar correo electrónico gratuito a los ciudadanos, deberán establecerse claramente en un contrato las relaciones entre la administración, que será normalmente el Responsable del Fichero, y el prestador de servicios,

que será, usualmente, Encargado del Tratamiento. En caso de otro tipo de relaciones contractuales, deberán aplicarse las normas sobre cesión de datos, especialmente la referida a la prestación del consentimiento, entre los órganos de la administración y los prestadores de servicios.

b) Cumplimiento de las normas sobre prestación del consentimiento y sobre la calidad y finalidad del dato en relación a los datos que puedan recogerse.

El artículo 6.2. de la LOPD establece, como excepción, que no será preciso el consentimiento inequívoco del afectado, cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Ahora bien, la cuestión a debatir se centrará precisamente en el principio de calidad y especialmente de finalidad del dato, perfectamente aplicable y en ningún caso contradictorio con lo que dispone el mencionado artículo 6. 2.

Será preciso que determinar que datos o si todos los datos de carácter personal recogidos a través de sitios WEB de la Administración Pública pueden formar parte de ficheros automatizados que almacenen datos para las funciones propias de los órganos administrativos en aplicación de la excepción del artículo 6.2. o bien, si para algunos de estos datos personales recogidos será necesario el consentimiento del afectado por no ser necesarios para el ejercicio de las funciones públicas.

c) Cumplimiento de la normas sobre comunicación y cesión de datos.

Independientemente de la aplicación del artículo 21 de la LOPD en los supuestos que proceda, el cual prevé que podrán ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra, la Administración pública electrónica deberá cumplir, con carácter general, los requisitos legales sobre comunicación de datos a terceros, especialmente el que se refiere a la prestación del consentimiento. Específicamente, será necesario el consentimiento para el tratamiento de datos de encuestas de opinión en el ámbito municipal o autonómico y para su adición a otros ficheros ya creados con datos de carácter personal.

d) La relación con los datos de los ficheros con finalidades estadísticas.

Finalmente, hay que tener en cuenta en relación a los ficheros estadísticos que gestionan las Administraciones Públicas como consecuencia de una actividad estadística oficial, que las normas de secreto estadístico de la Ley 12/1989, de 9 de mayo de 1989, de la Función Estadística Pública y de la legislación estadística de las Comunidades Autónomas, impiden la revelación de datos individuales y, por tanto, la incorporación de estos datos a los ficheros automatizados regulados por la LOPD de los que son responsables los órganos de la administración.

3.4. Referencia específica al régimen jurídico de Protección de Datos del Padrón Municipal de Habitantes

Con independencia de la problemática que plantea, y ha planteado en la práctica, la utilización de los datos personales del Padrón Municipal de Habitantes para según que finalidades y que no es objeto de este trabajo, la gestión electrónica del Padrón Municipal de Habitantes deberá tener en cuenta los siguientes aspectos sobre Protección de Datos:

a) La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal no permite la adición de nuevos datos personales recogidos por vía electrónica o de cualquier otro origen al Padrón Municipal de Habitantes, sin consentimiento del afectado.

b) Será preciso regular la cesión o el acceso por terceros a los datos del Padrón Municipal de Habitantes de acuerdo con las normas de protección de datos.

4. LA GESTIÓN DEL CORREO ELECTRÓNICO EN LAS RELACIONES CON LOS CIUDADANOS

4.1. La Administración electrónica y el correo electrónico

La implantación de la Administración electrónica conduce inevitablemente a que las relaciones entre ciudadanos y órganos de la administración se pueda llevar a cabo mediante el correo electrónico, desde las simples consultas o peticiones de información hasta la gestión y prestación de servicios públicos. En toda esta tipología de relaciones electrónicas entre órganos de la administración y ciudadanos, las administraciones públicas tendrán conocimiento de ciertos datos de carácter personal de los ciudadanos y en particular de la dirección de correo electrónico, con independencia de los mecanismos necesarios para que cuando se realice una operación a través de medios telemáticos se asegure la integridad del contenido y se autentifique al remitente y al receptor.

4.2. El correo electrónico como dato de carácter personal

En términos generales, el correo electrónico será un dato de carácter personal siempre que encaje en la definición de datos de carácter personal del artículo 3 de la Ley de Protección de Datos; es decir, que sea una información concerniente a personas físicas identificadas o identificables.

En consecuencia, la utilización del correo electrónico de los ciudadanos, personas físicas, por parte de las administraciones públicas deberá someterse a las normas de la Ley 15/1999, tanto por lo que se refiere a su recogida, a su tratamiento y a su comunicación o cesión, y también a la regulación de la Ley

34/2002, de 30 de julio, de servicios de la sociedad de la información y de comercio electrónico sobre el envío de comunicaciones electrónicas.

Datos del correo electrónico	Régimen jurídico del Dato	Régimen Legal LOPD
Correo electrónico que identifica o puede identificar a la **persona física**	Dato de Carácter Personal: **SI**	**Cláusula de Consentimiento para Tratamiento y Cesión**
Correo electrónico que identifica o puede identificar a la **persona jurídica**	Dato de Carácter Personal: **NO**	**No es necesaria la Cláusula de Consentimiento para Tratamiento y Cesión**
Correo electrónico que identifica o puede identificar a la **persona física como representante de una persona jurídica**	Dato de Carácter Personal: **NO** (exclusivamente en su consideración de representante de una empresa y sin menoscabo de otros derechos)	**No es necesaria la Cláusula de Consentimiento para Tratamiento y Cesión**
Correo electrónico que identifica o puede identificar a la **persona física profesional liberal**	Dato de Carácter Personal: **SI**	**Cláusula de Consentimiento para Tratamiento y Cesión**
Correo electrónico que identifica o puede identificar a la **persona física como profesional o empresario individual**	Dato de Carácter Personal: **NO** (exclusivamente en su consideración de empresarioy sin menoscabo de otros derechos)	**No es necesaria la Cláusula de Consentimiento para Tratamiento y Cesión**

* Cuadro incluido en la publicación “Las claves para la Gestión de Datos Personales en los Negocios Electrónicos”, © Jordi Bacaria – Ediciones Experiencia.

5. RÉGIMEN JURÍDICO DE LAS COMUNICACIONES POR VÍA ELECTRÓNICA

5.1. Regulación y aplicación de la Ley 34/2002 en materia de protección de datos

El artículo 21 de la Ley 34/2002, establece una prohibición en relación a las comunicaciones comerciales no solicitadas que se realicen a través de correo electrónico o por medios de comunicación electrónica equivalentes:

a) Norma general:

Como norma general, el precepto prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente.

b) Excepciones:

Permite el envío de comunicaciones publicitarias o promocionales en dos supuestos:

– Que hayan sido previamente solicitadas.

– Que hayan sido autorizadas expresamente por los destinatarios de las comunicaciones.

5.2. Aplicación de la Ley 15/1999 a las comunicaciones electrónicas

El artículo 19 y siguientes de la Ley 34/2002, regulan el régimen jurídico de las comunicaciones comerciales por vía electrónica, estableciendo el citado artículo 19, con carácter general, que les "será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo".

A continuación, el mencionado artículo especifica que se aplicará especialmente la Ley 15/1999, a:

– La obtención de datos personales en las comunicaciones electrónicas.

– La información a los interesados, titulares de los datos que reciban comunicaciones comerciales.

– La creación y mantenimiento de ficheros de datos personales.

Se habrá de entender, asimismo, que el resto de preceptos de la Ley Orgánica 15/1999, serán también de aplicación a las comunicaciones electrónicas, siempre que éstas se refieran o contengan datos de carácter personal.

5.3. El correo electrónico como dato de carácter personal: el doble régimen jurídico del artículo 19

Los artículos 21 y 22 de la Ley 34/2002, no determinan si se refieren al correo electrónico, el medio más usual para el envío de comunicaciones electrónicas, cuando es un dato de carácter personal o cuando no lo es, ni tampoco distinguen personas físicas o jurídicas. Por tanto, la prohibición del artículo 21 la deberemos entender referida a las comunicaciones comerciales electrónicas no solicitadas mediante correo electrónico:

– Sea o no el correo un dato de carácter personal.

– Sea el destinatario de la comunicación electrónica persona física o jurídica.

En todo caso, en términos generales, el correo electrónico será un dato de carácter personal, siempre que encaje en la definición de datos de carácter personal del artículo 3 de la Ley de Protección de Datos; es decir, que sea una información concerniente a personas físicas identificadas o identificables. A este respecto, debemos entender que el correo electrónico no será un dato de carácter personal:

– Cuando a través de la información que muestre no se identifique a la persona física o no sea posible identificarla.

– Cuando se refiera o dé información de una persona jurídica, es decir cuando se trate de un correo electrónico corporativo.

Del análisis de estos preceptos, se puede llegar a la conclusión que a los correos electrónicos les es de aplicación un doble régimen legal:

a) Comunicaciones electrónicas a través de correos electrónicos cuando éstos no constituyan un dato de carácter personal, pertenezcan a personas físicas o jurídicas.

En estos supuestos, se aplicaría el régimen jurídico y, si fuera el caso el régimen sancionador, de la Ley 34/2002.

b) Comunicaciones electrónicas a través de correos electrónicos cuando éstos constituyan un dato de carácter personal.

En estos supuestos:

– Se aplicaría el régimen jurídico y, si fuera el caso el régimen sancionador, de la Ley 34/2002 en relación a la prohibición del artículo 21 y sus consecuencias.

– Se aplicaría el régimen jurídico y si fuera el caso el régimen sancionador de la Ley Orgánica 15/1999 en cuanto a la recogida y tratamiento de datos de carácter personal.

5.4. Aspectos de Protección de Datos en el comercio electrónico

En el Título IV de la Ley 34/2002 dedicado a la regulación de los contratos celebrados por vía electrónica, no figura ninguna mención a la normativa sobre Protección de Datos de Carácter Personal. La referencia normativa a esta materia para los contratos celebrados por vía electrónica la encontramos en uno de los artículos que regulan las comunicaciones electrónicas, concretamente en el artículo 22, bajo el epígrafe general de derechos de los destinatarios de comunicaciones comerciales.

El artículo 22 establecía, específicamente, en su redacción original la regulación de las comunicaciones electrónicas durante la celebración de los contratos por vía electrónica. El precepto exigía el consentimiento del destinatario contratante del servicio antes de finalizar el procedimiento de contratación, en el caso que éste debiera facilitar su dirección de correo electrónico, durante el proceso de contratación o de suscripción a algún servicio, y el prestador pretendiera utilizarla posteriormente para el envío de comunicaciones comerciales.

Este consentimiento debería ser expreso, si interpretamos el artículo 22 de modo integrado con el régimen jurídico de las comunicaciones electrónicas de la Ley 34/2002.

Posteriormente a la entrada en vigor de la la Ley 34/2002, de 30 de julio, de servicios de la sociedad de la información y de comercio electrónico, se dictó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

El artículo 13 de la Directiva estableció una excepción a la necesidad del consentimiento expreso para el envío de comunicaciones comerciales por vía electrónica para los casos de clientes, cuya la dirección de correo electrónico se ha obtenido en el contexto de la venta de un producto o de un servicio, y se utilice para la venta directa de los propios productos o servicios de características similares del prestador de servicios.

5.5. La modificación de los artículos 21 y 22 de la LSSI por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones

La Disposición final primera. Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones regula la modificación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico en relación al régimen de las comunicaciones electrónicas cuando haya existido una relación contractual previa. Específicamente, se modifica el artículo 21 de la LSSI, que queda redactado en los siguientes términos:

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

A su vez, este precepto legal reconoce, asimismo, otros derechos de los destinatarios de comunicaciones electrónicas:

– Derecho a revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

– Derecho a la habilitación por parte de los prestadores de servicios de procedimientos sencillos y gratuitos para poder revocar el consentimiento que hubieran prestado.

– Derecho a que se les facilite información accesible por medios electrónicos sobre dichos procedimientos.