EL TRATAMIENTO INVISIBLE DE DATOS DE CARÁCTER PERSONAL EN INTERNET

ROBERTO YANGUAS GÓMEZ
Estudiante de Derecho
Universidad de La Rioja

SUMARIO

I. INTRODUCCIÓN

"¡Vaya, tenemos observadores! -exclamó K. en alta voz, dirigiéndose al inspector e indicando con su índice la ventana de enfrente-. ¡Váyanse! -les increpó. Sorprendidos, retrocedieron los tres con rapidez dos pasos hacia atrás. Los dos ancianos se escondieron detrás del hombre, que los ocultó con su corpachón, y a juzgar por el movimiento de sus labios, les habló algo, que la distancia les impidió oír. No obstante, no se ocultaron del todo, como si aguardasen el momento en que K. no pudiera verles, para volver a colocarse en la ventana"

KAFKA. F, *El Proceso*. Ed. Seix Barral. Madrid, 1987

La vida privada de las personas es hoy un bien muy preciado, tanto, que el legislador ha elaborado hasta la fecha un gran número de normas tendentes a la protección de la misma. El ser humano, como dijo Aristóteles, es un ser social: fuera de ello sólo puede ser un Dios o una bestia. Pero sin embargo, no se puede ser social las veinticuatro horas del día. Todos necesitamos, en algún momento, y en mayor o menor medida, disfrutar de la compañía de la soledad. Además, como ser libre, es el hombre quién debe elegir con quién quiere relacionarse y hasta qué punto. Ningún particular puede inmiscuirse en la vida de otro sin su consentimiento y menos aún si los propósitos no son desinteresados. De ello trata nuestro ensayo.

Las nuevas tecnologías, especialmente la informática a través de Internet, han configurado una gran red mundial de interrelaciones. Sin embargo, al igual que ocurre cuando vamos paseando por la calle, no todo el mundo tiene por qué saber quienes somos, o más aun, qué somos. En Internet, al igual que en la realidad física, debe abogarse porque sea la persona quién decida si quiere permanecer o no en el anonimato (siempre que no esté en juego el orden social).

II. EL OBJETO DE LAS NORMAS GENERALES RELATIVAS A LA PROTECCIÓN DE DATOS: DERECHOS Y BIENES JURÍDICOS PROTEGIDOS

1. Normativa aplicable y objeto de la misma.

Hemos de partir señalando cuales son las normas de cuyo análisis se nutrirá la mayor parte de este ensayo: en primer lugar, la Ley orgánica 15/1999, de Protección de Datos de Carácter Personal, de 13 de diciembre, (LOPD en adelante), norma que viene a transponer en el ordenamiento interno la Directiva 95/46/CE , de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y que deroga a la antigua Ley orgánica reguladora del Tratamiento Automatizado de Datos de Carácter personal, de 1992.

En cuanto al objeto de dicha normativa, y ciñéndonos al ámbito interno, la LOPD, tal y como se afirma en su artículo primero: "... 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 su honor e intimidad personal y familiar".

Sin embargo, pese a la teórica sencillez y claridad que emana de esta norma en relación al objeto protegido por la misma, nos encontramos, por el contrario, ante verdaderas dificultades a la hora de definir de manera pormenorizada cuál es el objeto al que se refiere. Dificultades que han tenido su reflejo en un extenso debate doctrinal, que vino a apaciguar en gran medida el Tribunal Constitucional en el año 2000 a través de la importantísima sentencia 292/2000 de 30 de noviembre.

2. Intimidad y privacidad.

Frente a la antigua concepción de que el derecho a la intimidad abarca la protección de las expresiones más interiores y reservadas del ser humano (filosofía, comportamiento sexual, etc.), esto es, de su vida íntima, podemos decir (consecuencia de la incidencia del transcurso del tiempo en los Derechos fundamentales positivizados en un momento histórico concreto), que intimidad se correspondería hoy con *privacidad*.

La privacidad abarca un espectro de protección más amplio que el núcleo al que hemos hecho referencia. Tal y como disponía la Ley orgánica 5/1992, reguladora del tratamiento automatizado de datos de carácter personal en su Exposición de Motivos, refiriéndose a privacidad e intimidad: "aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona (...), la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como

precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado." (1)

3. La autodeterminación informativa.

La fundamental STC 292/2000, de 30 de noviembre, a la que antes nos hemos referido, define la autodeterminación informativa como un derecho que "atribuye a su titular un haz de facultades que consisten en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos, *en relación con el tratamiento de sus datos personales* (2), cuya concreta regulación debe establecer la ley"

La LOPD tiene un campo de actuación mucho mayor que la LORTAD, un campo que abarca y se extiende sobre un conglomerado difuso de derechos y libertades. El legislador lo que pretende es defender tales derechos y libertades, y para ello, en lugar de concretar cuáles son éstos y atribuirles de manera unívoca un instrumento particular de protección, lo que hace es llevar a cabo una acción preventiva sobre el medio que puede vulnerar tales derechos, sean cuales sean. Y este medio no es otro sino el *tratamiento de datos personales*. Y es que el verdadero peligro no deriva de si se ponen en conocimiento datos de carácter íntimo o no. Sino de que la adecuada identificación (entrecruzamiento) de esos datos dispersos, que permiten las nuevas tecnologías, vinculándolas a un sujeto en particular, puede arrojar como resultado la indefensión o vulneración de determinados derechos.

III. DATO DE CARÁCTER PERSONAL: CONCEPTO

Poseer una concepción clara de dato de carácter personal no es algo que atienda con propósitos meramente doctrinales, sino que tiene una directa repercusión en la práctica, pues si no es posible determinar si un elemento constituye o no un dato de carácter personal, tampoco cabe discernir si éste se halla afecto a la regulación sobre protección de datos existente.

El artículo 3 de la LOPD se refiere a dato de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables".

---

1 Epecialmente interesante resulta en este sentido el Considerando 10 de la Directiva 95/46/CE, donde se dice que "las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho Comunitario." En este sentido, señala el art.8 CEDH que "Toda persona tiene derecho al respeto de su vida privada y familiar"

2 La cursiva es nuestra

Partiendo de esta definición podemos señalar, por tanto, dos presupuestos que definen a un dato como de carácter personal: 1) Que se trate de un dato concerniente a una persona física; y 2) Que tal persona física sea identificada o identificable

1. ¿Qué hemos de entender por dato concerniente a una persona física?

Por dato concerniente a una persona física hemos de entender, no sólo aquellos relativos a informaciones íntimas o especialmente características del sujeto en cuestión, sino a cualquier información que, por intranscendente o insignificante que pueda parecer, pertenece al fuero interno de la esfera privada de la misma (en el sentido que hemos definido privacidad anteriormente) [3].

Si *a priori* nos puede parecer esta una concepción muy amplia del ámbito a proteger, observamos que no se trata de un capricho del legislador, sino que, como ya hemos señalado con anterioridad, información cuyo tratamiento a simple vista puede parecer inocuo en cuanto a vulneración de derechos se refiere, estableciendo los apropiados vínculos puede llegar a servir para la elaboración de perfiles de personalidad, con el consiguiente peligro que, ahora sí, esto supone en relación con los derechos y libertades.

2. ¿Qué hemos de entender por Identificada o Identificable?

Significa que el dato personal no tiene porqué suponer identificación presente, basta con que lo sea en un futuro. Representa una posibilidad. Como señala VIZCAÍNO CALDERÓN [4] ha de entenderse, "no como necesaria identificación actual, sino como una posibilidad real de identificación".

El Considerando 26 de la Directiva 95/46/CE contiene una regla de interpretación a la hora de evaluar tal posibilidad real de identificación. Y concretamente señala que "para determinar si una persona es identificable hay que considerar el conjunto de los medios que pueden ser *razonablemente* utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona".

Es decir, apunta (como en su día lo hizo la propuesta de Directiva de 1990) a una *no* "inversión excesiva de tiempo y recursos humanos y económicos". Todo dato relativo a una persona que no cumpla este segundo presupuesto habrá de entenderse *disociado* [5]

[3] Ver apartado "Intimidad y privacidad".

[4] VIZCAÍNO CALDERÓN, M., *Comentarios a la LOPD*, pág.72. Madrid, 2001. Ed. Cívitas.

[5] Esto es, y con relación al art.3.f LOPD que habla del procedimiento de disociación, habrá de entenderse que el sujeto se halla en situación de anonimato.

IV. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Antes de comenzar la parte central de nuestro trabajo conviene recordar brevemente que LOPD viene a establecer una serie de principios cuyo respeto es presupuesto de partida para un correcto tratamiento de los datos de carácter persona.

La doctrina ha diferido formalmente en cuanto a la enumeración de tales requisitos. Sin embargo, todas las teorías vienen a converger en la idea que subyace de fondo, y que ha sido recogida con cierta nitidez (más aun que en los textos normativos que resultan ciertamente confusos y desorganizados en cuanto a la exposición se refiere), en el Considerando 28 de la Directiva 95/46/CE, y que enuncia lo siguiente: "Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetos originalmente especificados".

Así podríamos enumerar como principios fundamentales en el tratamiento de datos de carácter personal los siguientes: principio de finalidad predeterminada (art.4.1 LOPD); principio de proporcionalidad (art.4.1 LOPD); principio de lealtad (art.4.7 LOPD); principio de congruencia (art.4.2 LOPD); y principio de exactitud (art.4.3 LOPD).

Además, establece el Considerando 30 de la Directiva 95/46/CE que "para ser lícito el tratamiento de datos personales debe basarse (...) en el consentimiento del interesado". El Considerando 33 señala por su parte que,"los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito", y que "deberán constar de forma explícita las excepciones a esta prohibición". Ambos Considerandos constituyen el axis jurídico del principio de autodeterminación informativa.

V. INTERNET COMO FUENTE ACCESIBLE AL PÚBLICO

Entre las cuestiones más relevantes que debemos de plantearnos antes de entrar a estudiar a fondo los medios por los que se puede llegar a vulnerar el derecho a la autodeteminación informativa a través de Internet, se encuentra la pregunta de si hemos de considerar precisamente Internet como una "fuente accesible al público". De la contestación a esta pregunta dependerá de que jueguen en Internet, con plenitud o no, el derecho a la información previsto en el art.5 LOPD, y el principio de consentimiento del art.6 de la misma Ley. Puesto que si concebimos Internet como una fuente accesible al público no será necesario que se informe de forma expresa al interesado de la recogida de datos a el relativos sitos en la Red (art.5.5, párrafo segundo LOPD), ni que consienta en el tratamiento de los mismos (art.6.2 LOPD).

El artículo 3.j LOPD define como fuentes accesibles al público "aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de acceso público, *exclusivamente*, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación".

Nos encontramos ante un supuesto de *numerus clausus* [6], o enumeración taxativa, que supone que *sólo* y únicamente han de tener la consideración de fuentes accesibles al público: el censo promocional, los repertorios telefónicos y las listas de grupos de profesionales en los términos previstos, los diarios y boletines oficiales y los medios de comunicación.

La enumeración es clara. Sin embargo, la cuestión que planteamos en un principio no obtiene respuesta ciñéndonos únicamente a este precepto, pues si bien Internet no se halla recogido exclusivamente dentro de los supuestos tasados, no parecería, *a priori*, descabellado, incluirlo como parte integrante dentro de los *medios de comunicación*. No cabe duda de que Internet es un medio de comunicación en el sentido que permite transmitir grandes cantidades de información de una parte del globo a otra en muy pocos segundos. Sin embargo, sin atender a consideraciones puramente terminológicas, deberemos de saber cuál es el concepto jurídico de medio de comunicación a que se refiere la Ley 15/1999.

La respuesta a esta cuestión nos la ha dado nuevamente la Agencia de Protección de Datos (en adelante, APD), en una de sus respuestas a consultas planteadas recopiladas en su Memoria anual. En este caso, la respuesta se halla concretamente en la Memoria de la Agencia del año 2000 [7]. Al respecto señala la APD que "no se considera que la procedencia de los datos recogidos en Internet sea la de fuente accesible al público, siendo necesario, por lo tanto, la obtención del consentimiento inequívoco, específico e informado del afectado para realizar tratamientos con sus datos personales publicados en Internet, aunque estos se hayan publicado de forma que cualquier internauta pueda acceder a los mismos".

Así pues, y con esta contestación, la APD deja claro que en el caso de datos personales publicados en foros, grupos de noticias, *chats* o similares, éstos no podrán ser recogidos sin informar al sujeto a quién pertenecen, ni ser tratados sin su consentimiento. La tesis del principio de finalidad viene a reforzar este planteamiento, si tenemos en cuenta que la publicación de estos datos en los denominados "espacios públicos de internet" responde a motivos diversos, cuales son la posibilidad de recibir respuestas a *posts* (mensajes) publicados en foros, o entablar comunicación con otras personas. Pero en

[6] STSJ de Castilla y León, de 1 de octubre de 2002. RJCA 2002\1131

[7] *Memoria de la Agencia de Protección de Datos,* Ministerio de Ciencia y Tecnología. Madrid, 2002, pag.93.

ningún caso se adecuarán, por lo general, a la finalidad pretendida por el responsable de la recogida.

VI. LA DIRECCIÓN DE CORREO ELECTRÓNICO O E-MAIL COMO DATO DE CARÁCTER PERSONAL

La cuestión de si hemos de concebir la dirección de correo electrónico como dato de carácter personal no es una cuestión tampoco baladí, sino que, dependiendo de la respuesta, habremos de proyectar sobre la dirección e-mail las prebendas y disposiciones sobre protección de datos que indican las leyes internas y la normativa comunitaria. Este es un tema especialmente a tener en cuenta en el caso del *spam*, pues si entendemos que la dirección *de e-mail* no es un dato de carácter personal, en ese caso, el tratamiento del mismo con fines de prospección comercial no requerirá del sometimiento del responsable a determinadas pautas y deberes. Del mismo modo la venta o cesión de listas con millones de direcciones de *e-mail* también podrá se considerado como un acto perfectamente lícito. ¿Cómo se contesta a esta pregunta?

La respuesta corresponde nuevamente a la Agencia de Protección de Datos en una contestación a una consulta similar, concretamente a si "la venta o cesión de datos de un fichero que contiene direcciones de correo electrónico, debe ser considerada cesión de datos a los efectos de la ley" [8] (la LOPD se sobreentiende). La respuesta de la Agencia es clara: sí, ha de ser considerada cesión a los efectos de la ley. La APD lo justifica de la siguiente manera: existen direcciones e-mail que, en sí mismas, hacen identificable al sujeto, en cuanto en ellas se incluye el nombre del mismo, su edad, país o análogo. Sería el caso por ejemplo de la dirección roberto.yanguas@alum.unirioja.es. En este caso, la dirección e-mail contiene el nombre y primer apellido del titular de la misma. La organización en la que se encuentra integrado, en este caso la universidad de la Rioja. La posición que ocupa dentro de la misma, en este caso la de alumno. Y la zona geográfica a la que pertenece, en este caso España. Pues bien, en estos casos, la APD ha venido entendiendo que en aquellos supuestos en los que la dirección e-mail se refiera a aspectos particulares de un sujeto en concreto, que lo hagan identificable en cualquier faceta, la dirección e-mail habrá de ser considerada un *dato de carácter personal*.

Ahora bien, existen ocasiones en los que los datos mostrados no identifican al titular de la cuenta, incluso pueden identificar a otra persona distinta. O simplemente existen casos en los que la dirección e-mail está compuesta por caracteres alfa-numéricos que no representan ninguna realidad concreta, es el caso de direcciones como crz@mixmail.com, o bacci1000e@wanadoo.es. En estos casos, la APD ha dicho que habremos de estar a la norma general. Y la norma general no es otra que entender que un sujeto es identificable si

[8] *Memoria de la Agencia de la Protección de Datos,* Ministerio de Ciencia y Tecnología. Madrid, 1999, pág.127.

dicha identificación no supone un esfuerzo desproporcionado. Concretamente la APD ha dicho al respecto que "incluso en estos supuestos (a los que nos acabamos de referir), la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación mediante la consulta del servidor en que se gestione dicho dominio *sin necesidad de un esfuerzo desproporcionado* por parte de quien lleve a cabo dicha identificación"

Así pues, como vemos, para la APD la dirección de correo electrónico constituirá, en todos los casos, un dato de carácter personal. Sin embargo ha de ponerse en duda la correción de la anterior argumentación. Situémonos en el supuesto de una dirección alojada en una gran compañía proveedora de servicios de correo electrónico (por ejemplo *Hotmail*, cuyos servidores manejan millones de cuentas de correo diariamente). ¿Se habrá de entender que no constituye un esfuerzo desproporcionado el acudir a dicha compañía y solicitar información sobre el titular de la cuenta? La respuesta, a todas luces, parece negativa. A nuestro modo de ver, la APD ha acertado en el fondo del asunto, pues lo que se trata es de proteger del abuso a través del tratamiento de direcciones de correo electrónico. Sin embargo, la argumentación es pobre. Más correcto a nuestro juicio habría sido decir que, en tanto que en la cabecera del *e-mail* remitido queda registrada la dirección IP del ordenador del que partió, así como de los *host* intermedios, es este hecho más que suficiente para considerarlo como posible instrumento de identificación de una persona, y por ello es digno de toda la cobertura que ofrece la normativa reguladora sobre protección de datos.

VII. EL CHARLOTEO DEL NAVEGADOR (*CHATTERING*)

1. Consideraciones generales.

Cuando un usuario de Internet *navega* por la Red, lo que está haciendo es acceder a páginas alojadas en servidores [(9)] de todo el mundo. Para ello se emplea un tipo especial de software denominado *browser* o navegador. Algunos de los navegadores más conocidos son Internet Explorer, Netscape, Opera, Safari o Mozilla, entre otros.

Cuando el usuario introduce el URL (*Universal Remote Locator*) correspondiente, suma del protocolo y de la dirección antes visto, el navegador solicita al servidor donde está hospedada la página que nos la muestre, para que el usuario la pueda visualizar. En este

[9] Por *servidor* hemos de entender todo ordenador utilizado como intrumento para prestar un servicio. Por el contrario, el ordenador al que se dirige ese servicio se denomina *cliente*. Es por ello que Internet ha de ser considerado de manera global como una gran red multiservidor-multicliente, por cuanto los propios ordenadores actuales, al ser multiproceso, es decir, crear la ficción de que se desempeñan varias tareas a la vez, son capaces de funcionar simultáneamente como servidores y como clientes dependiendo de la actividad realizada (chatear, navegar, mantener una conversación oral, etc.)

proceso se transmiten datos a través del protocolo HTTP, datos a los que se les puede atribuir la calificación de datos de carácter personal, en el sentido ya estudiado [10]. Fundamentalmente son cinco, a saber:

1- En primer lugar se solicita la página que se quiere visualizar, a través de la instrucción GET. En dicha solicitud se señala el protocolo utilizado a fin de que el servidor pueda proceder en su actuación.

2- En la línea *User-Agent* se señala por lo general, el navegador utilizado y el sistema operativo del ordenador solicitante (Windows 98, Windows XP, BeOs, Linux...)

3- En una tercera línea se especifican los formatos aceptados para ser visualizados (texto plano, mapas de bits, imágnes JPGE o GIP, etc.). Sin embargo, en el caso del Internet Explorer y asimilados, se ha venido teniendo la "mala costumbre" de remitir al servidor que ciertos programas están instalados en el ordenador del solicitante (p.ej. Word o Excel)

4- En último término, algunos navegadores señalan el idioma especificado por el usuario para el navegador o para el sistema operativo.

5- Además, a través de este protocolo se pueden transmitir, sin que el usuario lo perciba, las denominadas *cookies* que estudiaremos más adelante

2. Interpretación jurídica.

Como vemos, al navegar por la Red se está vulnerando en la práctica totalidad de los casos la normativa sobre protección de datos.

Uno de los principios que hemos analizado en la parte introductoria como indispensables en todo tratamiento de datos de carácter personal es el principio de proporcionalidad. Aquí, no cabe duda de que el idioma, los programas que el usuario tiene instalados en su máquina o el sistema operativo utilizado, son datos de carácter personal por cuanto permiten identificar al usuario en varias facetas (idioma, preferencias en cuanto al uso de determinados productos informáticos, etc.). Y por otro lado, también resulta claro que la finalidad a que tiende el protocolo HTTP no debe ser otra que a posibilitar la visualización de páginas web en el computador del usuario. Técnicamente, para desempeñar tal función, sólo sería imprescindible la solicitud de la página a través de la instrucción GET. El resto de datos referidos **no son necesarios**. Por ello, y de acuerdo con el artículo 4.1 de la LOPD y 6.1.c de la Directiva 95/46/CE, tal acción estaría vulnerando el hecho de que "los datos sólo se podrán recoger para su tratamiento, cuando sean adecuados, pertinentes y no excesivos (*si bien sería discutible este punto*) [11] en relación con el ámbito y las finalidades... para las que se hayan obtenido".

Además, el usuario medio , ni tan siquiera sabe que su dirección IP está siendo transmitida en ese proceso. Es más, por regla general no es consciente, ni informado de

[10] Ver apartado "Dato de carácter personal: concepto".
[11] La cursiva es nuestra

ello, de que se están tratando datos que permiten identificarlo. Ni tan siquiera cuáles son esos datos, o que la dirección IP es uno de ellos, vulnerando así las disposiciones de los arts.5 y ss. LOPD, que constituyen el armazón básico de la defensa del derecho a la autodeterminación informativa en nuestro ordenamiento.

VIII. EL SPAMING

1. Spam: concepto y caracteres

En primer lugar, y antes de pasar a a analizar la realidad jurídica de este fenómeno, deberemos dar una concreta definición de *spam*, a fin de delimitar concretamente el objeto sobre el cual versarán los siguientes apartados. ¿Qué es el *spam* exactamente?

El término *spam* procede de Inglaterra, donde se utilizaba hace algunas décadas para designar a los trozos de carne, que, en las carnicerías, se regalaba a los clientes por las compras realizadas, salvo manifestación en contra de los mismos (**Sp**iced j**am**). En la actualidad, por **spaming** se ha venido entendiendo aquélla actividad, desarrollada en el espacio de Internet, consistente en el envío masivo de comunicaciones comerciales no solicitadas, por parte de una empresa. Suele ser habitual el falseo de los datos de cabecera del e-mail con objeto de que los emisores no puedan ser identificados posteriormente. Algunos autores han venido a distinguir entre *spam* y comunicaciones comerciales no solicitadas. Sin embargo, y a efectos de la nueva regulación, la definición dada de *spam* es perfectamente subsumible al supuesto de hecho regulado por la norma.

Debemos sin embargo aquí distinguir el *spam* de otras actividades de contenido semejante pero no idéntico y que, por tanto, no han de ser considerados ilícitos de acuerdo a la nueva normativa.

•***Permission marketing o marketing autorizado***: con este término se designa a la actividad realizada por las empresas, consistente en establecer una relación con el usuario de internet, a través de la Red, basada en una creciente confianza que se materializa a través de promesas cumplidas. En la práctica suele concretarse a través de concursos, ofertas, regalos o promociones, todos ellos buenos motivos para que el usuario consienta en el tratamiento de sus datos. Suelen ser campañas menos agresivas y con mejores resultados a largo plazo que el spaming.

Como están basados en el consentimiento del usuario, son perfectamente lícitas de acuerdo al art.13 de la nueva Directiva 2002/58/CE

•***Hoaxes***: se trata de un tipo de actividad tan difundida como el spam. Consiste en el envío de *e-mails* a través de la Red, que instan a quién las recibe, a que las reenvíe a sus contactos. En este caso la actividad se inicia con una o un número reducido de comunicaciones. Sin embargo su crecimiento es exponencial. El contenido de los mismos

suele ser historias (falsas en su inmensa mayoría), solicitudes de ayuda, odas a las más variopintas figuras o chistes.

Desde el punto de vista meramente jurídico cabría plantearnos si los *hoaxes* podrían ser considerados una conducta ilícita. Tanto la Directiva 2000/31/CE como la 2002/58, y en el plano del Derecho interno, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI a partir de ahora), y la nueva Ley General de Comunicaciones, hacen referencia a la conducta a regular como "comunicaciones comerciales no solicitadas" [(12)], o "comunicaciones no solicitadas con fines de venta directa" [(13)]. De lo que se deduce que una de las características inherentes a este tipo de conductas es el hecho de que en cuanto a su finalidad, tiendan a la venta de un producto o servicio, impulsadas por el ánimo de lucro. Es por ello, que las comunicaciones que carezcan de tal *animus* no incurrirán en el ilícito estudiado.

El fundamento jurídico de este tipo de actuaciones lo podríamos situar en el artículo 2.2 LOPD, cuando dice que "El régimen de protección de datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación... a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas"

2. *Opt-in* versus *opt-out*. La evolución de la normativa española y comunitaria.

A la hora de llevar a cabo la regulación sobre el envío de comunicaciones comerciales no solicitadas, el legislador tiene ante sí dos posibilidades en cuanto a la protección de datos y la prestación del consentimiento. Estas dos posibilidades se han venido a concretar en la doble política *opt-in /opt-out*, o lo que es lo mismo, de *consentimiento expreso* o *inclusión voluntaria* y de *oposición expresa o exclusión voluntaria*.

Cuando se remite a un consumidor, usuario de un servicio de correo electrónico, un e-mail de carácter comercial, es claro que, de acuerdo a lo que llevamos visto normativamente sobre protección de datos, éste deberá de consentir a tal envío de comunicación. Pues bien, este consentimiento, de acuerdo a la LOPD, podrá ser formalmente diferente en atención al contenido de los datos tratados. En este caso, parece claro que el *e-mail*, si bien constituye, como ya hemos visto [(14)], un dato de carácter personal, parece claro que tal dato no se encuentra entre los datos especialmente protegidos del art.7. Luego bastará en principio con el consentimiento tácito para que la publicidad pueda ser enviada a dicha dirección. Y es aquí donde surge la divergencia con el actual Derecho comunitario. La LOPD, como vemos, permite que se consienta tácitamente, es decir, que, siempre que se cumplan las previsiones dispuestas en el art.5 de la propia LO respecto al deber de información del responsable de los datos, se entenderá prestado el consentimiento salvo que el usuario se oponga expresamente. Es lo que se ha venido a

[12] Art.9 de la Directiva 2000/31/CE, y art. 21 de la LSSI
[13] Art. 13 de la Directiva 2002/58/CE
[14] Ver apartado "Dato de carácter personal: conepto".

conocer como política de *opt-out*, y que conllevaría en principio, la validez, en el ámbito de la protección de datos, del silencio positivo.

La política de la LOPD deriva de la Directiva 95/46/CE, norma comunitaria que transpone, y que posibilitaba a los Estados miembros de la UE el elegir entre consentimiento expreso y consentimiento tácito, con la excepción de los datos especialmente sensibles a los que hace referencia nuestra LOPD en su art.7, donde, en coherencia con lo señalado en el Considerando 33 de la Directiva, se requiere consentimiento explícito. Es decir, los Estados miembros, respecto a la generalidad los supuestos, podrían establecer si se debía prestar expresamente el consentimiento o cabía la otorgación tácita del mismo.

En 1997, la Directiva sobre venta a distancia [(15)] y en materia concreta de protección al consumidor, establece que el correo electrónico es una técnica de comunicación que puede utilizarse "a falta de oposición manifiesta del consumidor". Luego, nuevamente vemos aquí como el legislador comunitario opta por el sistema de opt-out en el ámbito de las comunicaciones electrónicas.

Tres años más tarde, la Directiva 2000/31/CE, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), en su art. 7.2 señala que, "sin perjuicio de lo dispuesto en las Directivas 97/7/CE y 97/66/CE, los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria ("opt-out") en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten". Es decir, la Directiva 2000/31/CE señala con carácter general la posibilidad de optar nuevamente a los Estados miembros, por la política de opt-out en el ámbito de las comunicaciones comerciales por *e-mail*, siempre en consonancia con lo dispuesto en la Directiva general 95/46/CE.

Sin embargo, va a ser en este punto donde la LSSI cambia el criterio mantenido hasta la fecha por el legislador interno y opta por una política de *inclusión voluntaria*.

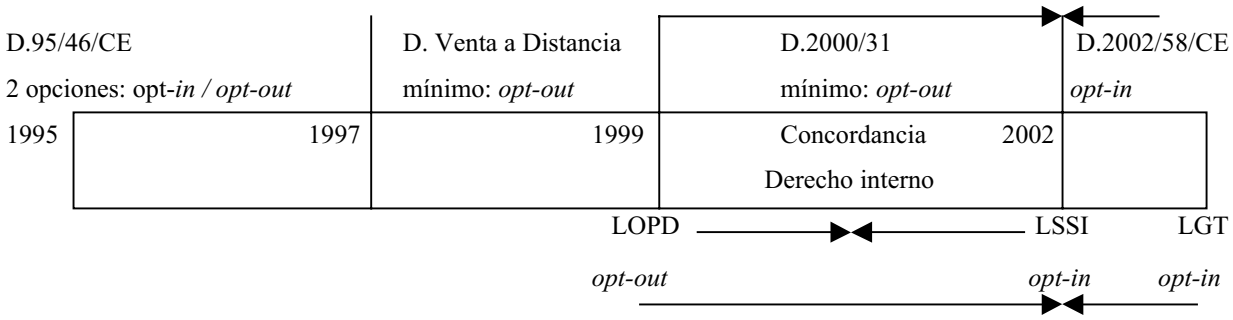
Por si el caos normativo no fuera suficiente, finalmente, en el año 2002, Parlamento Europeo y Consejo, acuerdan, mediante el procedimiento de codecisión, la aprobación de la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Es en este momento, cuando, debido al exponencial incremento del *spam*, a las dificultades que conlleva una doble regulación [(16)] y a las negativas repercusiones que esto tiene en el mercado

[15] Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de venta a distancia

[16] Hasta ese momento tan sólo Austria, Dinamarca, Alemania, Finlandia e Italia practicaban una política de *opt-in*, lo que suponía para los prestadores de servicios numerosos problemas a la hora de orientar sus

(especialmente en las transacciones comerciales vía Internet), decide cambiar de orientación y unificar el derecho comunitario. Así, en el artículo 13 de Directiva se establece que: "sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana, fax o *correo electrónico*, con fines de venta directa *respecto de aquellos abonados que hayan dado su consentimiento previo*". Es decir, se establece con carácter general y aplicable para todos los Estados miembro, la exigencia del consentimiento expreso (opt-in) en el ámbito de las comunicaciones comerciales por e-mail, desterrando así, al menos en teoría, las prácticas consagradas hasta la fecha y las denominadas Listas Robinson.

Para adecuarse a lo anterior, y tras cierta tardanza, el legislador interno ha transpuesto la directiva mediante la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT a partir de ahora), cuya Disposición Adicional Primera amplía el antiguo y ratifica lo ya dispuesto en el art.21 de la LSSI (fundamento del consentimiento expreso) reafirmando su postura de asunción del derecho comunitario.



Cabría destacar aquí, por último, y en cuanto a iniciativa comunitaria se refiere, una comunicación de la Comisión de 22 de abril de 2004, en la que se proponen "acciones de aplicación y cumplimiento de la legalidad vigente, de autorregulación y acciones técnicas y de sensibilización" [17]. Si bien es cierto que dicha comunicación no tiene vinculación normativa, es probable que en un periodo relativamente corto de tiempo dicha opción se vea materializada normativamente a través de nuevos instrumentos o modificaciones de la Directiva 2002/58/CE.

3. Problemática normativa

Lo que nos interesa es, desde luego, resolver el nudo gordiano planteado, y para ello vamos a intentar ir paso por paso:

---

actuaciones, sobre todo si tenemos en cuenta que en numerosísimas ocasiones el e-mail por si sólo no permite conocer la nacionalidad de la persona a que pertenece el mismo.

[17] <www.iustel.com>, 24 de marzo de 2004.

a) En el periodo que media entre la Directiva 95/46/CE y la Directiva 2000/31/CE, legislador comunitario e interno van de la mano y no se contradicen en modo alguno (al menos en este ámbito, pero si en otros como veremos más adelante).

b) Desde la transposición de la Directiva 2000/31/CE, hasta la aparición de la Directiva 2002/58/CE el problema residía en la existencia de dos normas internas, la LOPD y la LSSI, que pese a estar ambas amparadas por el legislador comunitario, se contradecían entre sí. En este periodo, por tanto, primaría la LOPD, ya que la disposición final segunda de la misma incluye los arts. 6 y 7, objeto de conflicto, dentro de los de carácter orgánico. Y dado que el objeto de regulación (especialmente en lo referido al art.5.5, segundo párrafo LOPD) es el mismo, será la Ley Orgánica quien hayan de primar, en última instancia, sobre la ley ordinaria [(18)]. Así por tanto, respecto a las comunicaciones comerciales vía e-mail cabría entender la existencia de una política de exclusión voluntaria, que ampararía las prácticas de enviar publicidad si el interesado es informado y no se pronuncia al respecto.

c) Tras la Directiva 2002/58/CE se produce una incompatibilidad en lo relativo a las comunicaciones comerciales por *e-mail*. Por tanto, dado que se trata de una norma precisa e incondicional cuyo plazo de transposición había el 31 de octubre de 2003, habría que aplicar en este periodo la teoría general del Derecho comunitario para ver si, en su caso, podría hacerse valer en algún caso lo dispuesto en ella (norma precisa e incondicional, aplicable sólo a relaciones verticales y ascendentes con el Estado, no transpuesta en plazo)

Cabría aun plantearnos es si era necesaria la transposición de la Directiva 2002/58/CE o bastaba con lo dispuesto en la LSSI. Podríamos inclinarnos a pensar, en principio, que será necesaria al menos una reforma en la Ley orgánica que establezca la necesidad de consentimiento expreso, aparte de para los supuestos recogidos en el art.7, para las comunicaciones comerciales vía correo electrónico; y que en tanto eso no se haya producido, no podría alegarse como fundamento jurídico la LSSI como norma transpuesta. No obstante, todo ello parece resolverse mediante la citada LGT, si bien es cierto que nos hallamos ante los mismos interrogantes y discordancias internas que en el supuesto anterior.

La realidad es que nos encontramos aquí ante un problema jurídico de difícil solución, incluso podríamos atrevernos a decir que carece de solución hasta que no se pronuncien los tribunales, y por tanto opinable. De este modo, tampoco resultaría absurdo ni mucho menos, entender que la LSSI es apta como norma que transpone la Directiva, y que el problema en este caso ya no es a nivel comunitario, sino a nivel interno [(19)]

[18] En este sentido el Ministerio de Ciencia y Tecnología vino a decir en la FAQ de su página web <www.mcyt.es> que, respecto del consentimiento sería aplicable lo dispuesto en la LOPD y no lo dispuesto en la reciente LSSI

[19] A modo de breve recordatorio, y para no perdernos, señalar que pese a que el art.30 de la LOPD sobre el tratamiento con fines de publicidad y prospección comercial no tiene el rango de orgánico por no estar sujeto a reserva de acuerdo a la Disposición final segunda, *estricto sensu*, de la misma ley; sigue habiendo contradicción insalvable entre los arts. 5.5 y 6.2 LOPD y 13 Directiva 2002/58/CE. Y de ahí toda la polémica suscitada

4. La nueva capacidad sancionadora de la APD en materia de Spam.

La otra gran reforma que plantea la nueva Ley General de Telecomunicaciones y que ha pasado bastante inadvertida es la posibilidad que se le otorga a la Agencia de Protección de Datos en materia de *spam*. Hasta la entrada en vigor de la nueva ley, el artículo 43 de la LSSI señalaba, en su número primero, que: " la imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología, y en el de infracciones graves y leves (caso del *spam* de acuerdo al artículo 38.3.b y 38.4.d) [(20]Al respecto cabe mencionar que la nueva Ley General de Comunicaciones también reforma ambos apartados incluyendo el inciso "...desinatarios que no hayan autorizado su remisión *o se hayan opuesto* a ella...", que, a nuestro juicio, vuelve a suponer un ejemplo de deficiente técnica legislativa por cuanto su interpretación autónoma, sin tener en cuenta todo lo dicho hasta ahora, podría dar lugar a grandes equívocos.[)], al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información" (SETSI). Sin embargo, el número cinco de la Disposición final primera de la nueva ley reforma el apartado segundo del artículo 43 LSSI, estableciendo que, "...corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3.b) y 38.4.d) de esta ley". Es decir, los referidos al *spam*.

Resumiendo, hasta la entrada en vigor de la nueva ley era el SETSI quién se produce de respecto de la única resolución sobre *spam* de la que tenemos conocimiento en España (Casp David M.E contra "Guía de Empresas en Internet S.L."). Y es que, la resolución sancionadora de la APD es anterior a la entrada en vigor de la nueva LGT. Así pues, quién debiera haber conocido del asunto, y sancionado en su caso es el SETSI. Nuevamente nos enfrentamos a una difunción jurídica.

IX. HIPERVÍNCULOS INVISIBLES

Como su propio nombre indica, los *hipervínculos invisibles* son canales de transmisión de datos que el usuario de Internet no percibe y a través de los cuales se está vulnerando su derecho a la autodeterminación informativa. Hay dos grandes modalidades: hipervínculos invisibles que actúan en la navegación e hipervínculos invisibles que actúan a través de programas.

[20] Dispone el art.38.3.b que: "son infracciones graves... el envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a destinatarios que no hayan autorizado o solicitado expresamente su remisión o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando éste no hubiera solicitado o autorizado su remisión". En tanto que el art.38.4.d señala que "son infracciones leves... el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan solicitado o autorizado expresamente su remisión, cuando no constituya infracción grave".

1. Hipervínculos invisibles que actúan en la navegación.

Dentro de estos, hemos de distinguir a su vez dos subtipos, los *hipervínculos invisibles en sentido estricto*, y los denominados *bugs*.

1.1 Hipervínculos invisibles en sentido estricto.

Cuando se solicita a través del navegador una página web, en ocasiones, los datos transmitidos no se dirigen a un único servidor, concretamente al que aloja la página. Sino que en ocasiones, dentro de las páginas hay espacios en blanco, vacíos de contenido, que el responsable de los contenidos alquila a otra empresa [(21)] para que ésta proyecte en ellos su publicidad [(22)], a cambio de una contraprestación económica.

El ejemplo paradigmático es el de los *buscadores* de internet. En la práctica, cuando un usuario ingresa en la página principal de Google [(23)] y escribe un texto como parámetro de búsqueda (por ejemplo "Fernando Alonso"), lo que sucede es que el resultado de la misma corresponde a una dirección similar a esta:

http://www.google.es/search?q=%22**Fernando+Alonso**%22&ie=UTF-8&oe=UTF-8&hl=es&btnG=B%C3%Busqueda+en+Google&meta=lr%Dlang_es

Como vemos, dentro de la dirección de respuesta se incluyen los términos de nuestra búsqueda, que han sido empleados para localizar en las páginas que el buscador ha indexado, a fin de poder proporcionar el servicio, la información correspondiente. Sin embargo, y desde el prisma de la protección de datos, ocurre que en numerosas ocasiones ese *path* o cadena de búsqueda, o aun incluso la dirección de respuesta, es enviada automáticamente a un tercero con quién el buscador tiene contratado, quien, de acuerdo a los términos extraídos de la dirección mostrada (en este caso *Fernando+Alonso*), busca en su propia base de datos la categoría que más se aproxima a ellos a fin de enviar al espacio en blanco contratado la publicidad correspondiente.

No obstante, pese a lo gráfico del ejemplo cabe decir que no solamente a través de los buscadores se lleva a cabo este tipo de actividad, sino que son, por desgracia para el usuario, numerosas las páginas que contienen este tipo de hipervínculos.

1.2. Web Bugs ("bichos del web").

[21] Notese que nos estamos refiriendo siempre a empresas, entendiendo por tales cualquier entidad o persona física, que actúe movido por propósitos comerciales

[22] El caso paradigmático es el de los denominados portales de internet que proporcionan al usuario un enlace a un gran número de servicios, o el de los grandes buscadores como Google o Yahoo.

[23] <www.google.com>

También conocidos como "Bacon GIFs", "Invisible GIFs", "Clear GIFs" o "1-by-1 GIFs"[24], los *web bugs* son imágenes en formato GIF, de un reducido tamaño (la mayoría de 1 pixel cuadrado, que es el tamaño mínimo que puede mostrar un monitor), y en muchas ocasiones transparentes. La consecuencia de ello es que pasan desapercibidos para el usuario, son inapreciables.

Los *web bugs* se vienen a utilizar de dos modos distintos: asociándose a un archivo (documentos de word, excel, etc.); o bien asociándose a una página web. En ambos casos la imagen no está incluída dentro de dichos documentos o páginas web. En realidad, la imagen se halla alojada en un servidor de Internet. Lo que existe en la página o documento es un mero vínculo (una especie de acceso directo) cuya funcionalidad consiste en acceder al servidor donde está alojada la imagen y descargarla.

¿Qué se consigue con eso? Pues en el caso de los *web bugs* asociados a documentos, permite conocer (siempre que el ordenador se halle conectado a la Red), en qué fecha y hora han sido abiertos esos documentos, la IP del ordenador donde se han abierto y todos los datos propios del charloteo de navegador que ya hemos visto. En el caso de los *web bugs* situados en páginas web, permiten conocer, además, la página web visitada. La utilidad para el responsable del *web bug* es enorme. A través de estos datos puede llegar a saber cuáles son las páginas web más visitadas a fin de contratar publicidad con ellas; cotejar el éxito que ha tenido una campaña de *spam* (los gestores de correo suelen tener activada por defecto la vista preliminar del documento); e incluso elaborar un seguimiento de los hábitos de navegación de un mismo sujeto.

A) Aspectos Jurídicos

a) Normativa aplicable.

Antes de pasar a debatir sobre el fondo del asunto, deberemos señalar cuál es la normativa aplicable en relación con estas nuevas figuras (incluido el *adware* del que hablaremos en el posterior apartado). La Directiva 2002/58/CE afecta al tratamiento de datos en el sector de las comunicaciones electrónicas [25]. Cabría plantearnos por tanto si la normativa en ella es aplicable a los supuestos tratados..

La Directiva 2002/21/CE , relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, de 7 de marzo de 2002, define en su artículo 2.c *servicio de comunicaciones electrónicas* como el "prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos".

[24] <www.bugnosis.com>

[25] A diferencia de la Directiva 97/66/CE a la que deroga, que se refería al sector de las telecomunicaciones

De la anterior definición se deriva que los servidores de contenidos transmitidos a través de redes y servicios de comunicación electrónica no pertenecerán al ámbito de la Directiva 2002/58/CE. Es por ello, que en el caso de los hipervínculos invisibles dirigidos al envío de pancartas personalizadas en atención a los gustos o intereses del usuario (hipervínculos invisibles en sentido propio y *adware*), deberemos de atenernos únicamente a lo dispuesto por la normativa general, y concretamente por la LOPD. Sin embargo, en el caso de los *web bugs* y las *cookies* [(26)], será aplicable lo dispuesto en la Directiva 2002/58/CE [(27)]

b) Tratamiento de datos personales a través de hipervínculos invisibles en sentido estricto (con finalidad de envío de banners).

Podemos plantearnos si este tratamiento invisible de datos personales esta permitido por la actual legislación sobre protección de datos.

Todo tratamiento debe respetar los principios a que tantas veces hemos aludido ya, de finalidad, congruencia, proporcionalidad, exactitud, lealtad, etc. Asimismo se debe respetar el derecho a la información y el principio de prestación del consentimiento.

Por otra parte, no hemos de olvidar que en tanto se está enviando información de carácter personal (dirección IP, páginas visitadas, etc.) a un tercero nos hallamos ante un supuesto de *cesión de datos*, en el sentido del art.3.i LOPD [(28)].

Nos encontramos por tanto ante un problema complejo. En primer lugar, y antes de analizar si la cesión a los terceros es lícita o no, tendremos que comprobar si el prestador de servicios está legitimado para tratar los datos de carácter personal del usuario, entre los que se encuentra, al menos, su dirección IP. Para proceder a continuación a examinar si, partiendo de la lícitud del tratamiento, la cesión de datos es posible. Se tratan, como vemos de dos presupuestos cumulativos, la legitimidad de la cesión sólo será posible en tanto en cuanto el tratamiento previo sea lícito.

i) La legitimidad del tratamiento:

Cuando accedemos a una página web, lo que pretendemos es visualizar el contenido de la misma. Para ello, el servidor al que dirigimos nuestra solicitud debe conocer cuál es la dirección IP del solicitante, y cuál es la concreta solicitud. Estos son los requisitos mínimos para que la relación sea funcional.

---

[26] *Vid intra*

[27] En este mismo sentido Documento de trabajo: *Privacidad en internet: enfoque comunitario integrado de la protección de datos en línea*, aprobado por el Grupo de Trabajo sobre protección de datos del artículo 29, el 21 de noviembre de 2000, WP 37, 5063/00/ES/final, pág.28.

[28] El art.3.1 entiende por cesión o comunicación de datos "toda revelación de datos realizada a una persona distinta del interesado"

El art.5 LOPD como ya hemos visto, exige la previa información al interesado respecto al subsiguiente tratamiento de los datos de carácter personal a él vinculados. En este sentido mayoría de los navegadores actuales [(29)] advierten antes de realizar ninguna búsqueda que los datos van a ser transmitidos por un canal de comunicación abierto que no es completamente seguro, preguntando al usuario si desea continuar. Y por su parte, el art.6 exige el consentimiento del interesado respecto del tratamiento de los datos personales a él vinculados.

Respecto del derecho a la **información**, la problemática que supone, en cuanto el propio usuario no sabe qué datos se transmiten ni el carácter de los mismos, ya fue objeto de análisis en el apartado dedicado al charloteo del navegador [(30)]. Por otro lado, el único pronunciamiento al respecto en una norma comunitaria (en sede de Derecho interno aplicable no ha habido ninguna hasta el momento), ha sido el que se lleva a cabo en el Considerando 24 de la Directiva 2002/58/CE. En él se señala textualmente que "Los denominados "programas espía" (*spyware*), *web bugs*, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. *Sólo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados*". El Considerando en sí no aporta nada nuevo respecto a la Directiva general, y al no tener plasmación efectiva dentro del articulado, tampoco tiene fuerza normativa de aplicabilidad. Seguimos por tanto ante una materia no regulada. Ahora bien, el hecho de que el legislador se haya preocupado por incluir este inciso en la Directiva debe ser entendido al menos como una manifestación de intencionalidad, y por tanto, *debería* ser considerado por los Estados miembros como un criterio a tener en cuenta, en consonancia con el principio general de lealtad comunitaria, que tiene su fundamento en el art.10 TCE [(31Los Estados miembros se abstendrán de todas aquellas medidas que puedan poner en peligro la realización de los fines del presente Tratado")].

En el caso del **consentimiento**, el art.6.2 de la LOPD establece que "No será preciso el consentimiento cuando... se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento". En este caso, aunque el acceso a las páginas donde se hallan los hipervínculos invisibles, no suele conllevar ninguna contraprestación por parte del usuario, éstas se lucran a través de la financiación de terceros. el TJCE ha venido interpretando, a propósito, en este sentido, que "no es necesario que la remuneración vaya a cargo del

[29] Como ejemplo, el navegador Opera, cuando accedes a determinadas páginas te pregunta: "Send form without encryption?"; o el Internet explorer: "Va a abandonar una zona segura de internet. ¿Desea continuar?"

[30] Ver apartado "El charloteo del navegador (*chattering*)

[31] Dispone el art.10 TCE que: "Los Estados miembros adoptarán todas las medidas generales o particulares apropiadas para asegurar el cumplimiento de las obligaciones derivadas del presente Tratado o resultantes de los actos de las instituciones de la Comunidad. Facilitarán a esta última el cumplimiento de su misión.

beneficiario del servicio, pues también puede corresponder, por ejemplo, a los anunciantes" (32).

Ahora bien, aunque estemos ante una relación con tales características la pregunta es: es necesario este tipo de actividad para su mantenimiento o cumplimiento? La respuesta parece no dejar lugar a dudas: en el caso de la dirección IP y de la solicitud, técnicamente sí.

ii) La cesión de datos:

El artículo 11 de la LOPD establece en su apartado primero que "Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". En términos del art.3.i, toda revelación o manifestación de los datos a un tercero constituye una cesión de los mismos.

El artículo 11 LOPD establece, por tanto, dos requisitos para que la cesión sea legítima: en primer lugar que dicha comunicación responda al cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y en segundo lugar, que cuente con el previo consentimiento del interesado.

Sin entrar al debate acerca de si el tratamiento invisible con fines de financiación o análogos cumpliría el primero de los requisitos; baste decir que en el caso de los hipervínculos invisibles, es una característica a ellos inherente el no requerir el consentimiento del afectado, dado que el tratamiento se realiza entre el momento de solicitud de la página web o de la imagen de descarga y el momento de respuesta o apertura del documento. Además también es una característica que los define (sobre todo en el caso de los *web bugs*), el tratar de proceder con la máxima discreción posible, a fin de que el usuario ni tan siquiera perciba su presencia (33), vulnerando así el principio de tratamiento leal. Es por todo ello que podemos afirmar que *toda* utilización de hipervínculos invisibles en la navegación vulnera en todo caso el apartado primero del artículo 11 LOPD y ha de considerarse, por tanto, y sin entrar en otras valoraciones, ilícita.

c) Tratamiento de datos de carácter personal a través de web bugs

Además de considerar válido para los *web bugs* todo lo dicho acerca del tratamiento efectuado mediante hipervínculos invisibles en sentido estricto, y dado que también se aplicaría en este caso la Directiva 2002/58/CE, hemos de establecer una especialidad. Esta especialidad viene establecida en el art.5 de la Directiva y se refiere a la confidencialidad

[32] Asunto C-109/92 Wirth (1993) Rec I-6447, 14.

[33] Clara prueba de ello es que los profanos en la materia, pero que sin embargo hayan tenido alguna vez un acercamiento práctico al fenómeno de la navegación en Internet, desconocen su existencia en un altísimo porcentaje.

de las comunicaciones. Concretamente dispone lo siguiente: "Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público".

Entre los datos de tráfico a que se refiere la Directiva, se encuentra la dirección IP [(34)]. Si bien es cierto que la Directiva no está transpuesta en nuestro ordenamiento por el momento, sí que parece claro que la finalidad queda determinada, y no es otra que la confidencialidad de las comunicaciones y de los datos de tráfico asociados a ella. Por tanto, en el caso de los *web bugs*, al protegerse la dirección IP, se estaría, de modo indirecto, imposibilitando la utilización de dicho instrumento, pues, como ya hemos dicho, es el conocimiento de la IP el único medio que posibilita efectuar el seguimiento.

Para finalizar con los *web bugs* cabría preguntarse si sería aquí aplicable lo dispuesto en el art.5.5 LOPD. Dicho artículo establece que "[No] será de aplicación lo dispuesto en su apartado anterior... cuando el tratamiento tenga fines históricos, estadísticos o científicos". Es decir, cabría preguntarnos aquí si los *web bugs* serían legítimos cuando no hayan sido recabados directamente del interesado (art.5.4 LOPD) pero fueran únicamente instrumentos utilizados para comprobar la afluencia a páginas webs o el éxito de determinadas campañas publicitarias. La respuesta es, si nos atenemos a la letra de la norma, afirmativa, pues en este caso, los *web bugs* estarían desempeñando una función análoga a la de un contador (counter), que no hace sino registrar la IP, hora y día de acceso a la página web donde se halla ínstito. Sin embargo, debido a la inobservancia del principio de lealtad del art.4.7 de la misma ley, difícilmente podemos considerar esta práctica aún y con este fín, lícita por cuanto utiliza medios claramente fraudulentos o desleales. Como vemos la respuesta a estas preguntas está en muchos casos sujeta a diversas interpretaciones y no siempre es cerrada.

2. Hipervínculos invisibles que actúan a través de programas: el Adware.

Se entiende por ***adware*** todo software o parte de un **programa que permite enviar publicidad al usuario del mismo a través de ventanas, pop-ups, banners (pancartas) o análogos**. Para ello, los creadores del programa lo que hacen es incluir **partes de código** que desempeñan dichas funciones y que, en muchas ocasiones, **no pueden ser eliminadas sin que el programa deje de funcionar en su conjunto**. Lo más común a este respecto es

[34] El Considerando 15 señala al respecto que "Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cuál se transmita la comunicación a edectos de llevar a cabo la transmisión."

En el mismo sentido, el art.2.b define como *datos de tráfico* "cualquier dato tratado a efectos de conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"

emplear "archivos dll" (*dynamic library* o librerías dinámicas) encargadas, como módulo autónomo, de llevar a cabo la función publicitaria.

Los resultados y el procedimiento por el cual se vulnera el derecho a la autodeterminación informativa son similares a los de los hipervínculos invisibles y *web bugs*, pues también conllevan la cesión de datos de carácter personal a terceros sin la advertencia del usuario. La diferencia estriba sin embargo en el caso de los programas informáticos en que aquí la cesión de datos no se produce en un espacio temporal tan próximo como en aquéllos, y además, en este caso se informa al usuario de los diferentes derechos y deberes que tiene al ejecutar el programa a través de los denominados *contratos de licencia de uso*, de manera previa a la instalación en sí del propio. Aquí entraría en juego la regulación sobre propiedad intelectual [(35)] y sobre Condiciones Generales de la Contratación, y es un tema que escapa con creces de las aspiraciones del presente artículo. Sin embargo, y en cuanto a lo que nos interesa, el art.5.2 de la LOPD, en relación con el derecho a la información en la recogida de los datos, dispone que "cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior", esto es, de la existencia de un fichero; del carácter obligatorio o facultativo de las preguntas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación cancelación y oposición; y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

No parece descabellado, en este sentido, concebir el contrato de licencia de uso (*License Product Agreement*), como un formulario donde se le da la oportunidad al responsable del programa de ejercitar el deber de información que la ley recoge. Por tanto, desde una perspectiva estrictamente jurídica, un contrato de licencia de uso, claro, legible, donde se informe de manera expresa, precisa e inequívoca que se van a tratar datos de carácter personal, incluso de que van a ser cedidos a terceras partes a fin de que estos puedan enviar propaganda comercial al ordenador del usuario, y la aceptación de la licencia por parte del mismo, estaría respetando la normativa de protección de datos, cumpliría los principios de congruencia y proporcionalidad, y respetaría el derecho y deber a la información del usuario y responsable, y de prestación del consentimiento del interesado.

Sin embargo, y pese a lo anterior, en la práctica esto rara vez ocurre. La información nunca se adecua a los requisitos legales, más bien se formula de manera confusa y ambigua, omitiéndose alguno o todos los extremos exigidos por el art.5.1 LOPD.

Además, y respecto del requisito de la utilización de los formularios *claramente legibles* del art.5.4 LOPD, es algo que rara vez se respeta. Los contratos de licencia de uso suelen ser oscuros de entendimiento, extremadamente largos, reiterativos y poco precisos, además de que están formulados en forma de contrato de adhesión y constantemente vulneran los dispuesto al respecto, en relación con la regulación de las condiciones

[35] Real Decreto Legislativo 1/1996 por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. BOE núm. 97, de 22 de abril de 1996

generales de la contratación [36]. Materialmente se formulan a través de ventanas cuya maximización no es posible y donde el usuario debe, si quiere leer toda la información, desplazar el texto mediante el ratón o el teclado, en una larga y tediosa tarea.

3. Un supuesto particular: el Espyware.

3.1. Aspectos técnicos.

Los *spyware* son aplicaciones que envían información vía Internet al explotador de los mismos. Normalmente se componen de un núcleo funcional, que representa una verdadera utilidad para el usuario (programas de descarga, juegos, reproductores multimedia...), y, al igual que en el caso del *adware*, de un módulo encargado de recopilar información. Este módulo desarrolla su actividad en "background", esto es, en segundo plano, oculto por así decirlo. Y tan sólo podemos saber de él a través de *firewalls* (programas que recogen la procedencia de los datos entrantes y salientes del ordenador), o a través de un monitor de procesos, que nos muestre todos los procesos que están corriendo en ese momento bajo el sistema operativo.

Los responsables de seguridad de Symantec [37], en un Libro blanco (*white paper*) de 2001 [38], vienen a definir el *spyware* como "aplicaciones que envían información a través de Internet a los responsables, con propósitos comerciales y sin clara notificación a los usuarios". Por lo general, señalan, el *spyware* es generalmente *freeware* [39] o *shareware* [40], y que la recogida de información no suele mencionarse antes de la instalación a fin de hacer el programa más atractivo para los usuarios.

Symantec, al igual que se ha venido haciendo en gran parte de los círculos relacionados con la materia, incluye dentro de los "programas espía", el adware. A nuestro juicio, si bien ambos tipos de *software* tienen cierto parecido, existen algunas diferencias que nos hacen estudiarlos de manera autónoma, sobre todo en atención a la finalidad (el adware es un tipo de *spyware* orientado al envío de la publicidad, pero existen otros tipos de programas espía que no tienen ese fin).

---

[36] A este respecto, la norma reguladora básica por excelencia en el derecho español es la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación. En concreto, los arts.5.4 y 7.b, en relación con el art.10.1.c de la Ley 26/1984, de 19 de julio, general para la defensa de los consumidores y usuarios, cuando se trata de relaciones entre empresas de comercialización de software y consumidores particulares. Y todo ello en relación con el denominado control de inclusión de cláusulas en las Condiciones Generales de la Contratación

[37] Una de las empresas más importantes a nivel mundial dedicada al desarrollo de software "de defensa" frente a los peligros informáticos (Norton antivirus, Norton Firewall, Norton Security, etc.)

[38] "The dangers of *spyware* by André Post. Symantec Securuty Response"

[39] Software gratuito

[40] Software con limitaciones en su uso. Estas limitaciones pueden existir en cuanto al tiempo de uso, o al número de veces que puede abrirse el programa. En ocasiones consisten en que no todas las opciones que te permite realizar la versión "completa" del programa pueden llevarse a cabo. Incluso cabe el supuesto de que durante su uso aparezcan molestas ventanas o dibujos que incordian al usuario en el desarrollo de su actividad.

La revista *Time*, de 31 de julio de 2000 publicó un reportaje titulado "Cómo proteger tu intimidad: ¿quién te observa?". En este artículo se refirió a los programas espía con una denominación ciertamente irónica: la de "programas E.T", porque según decía el autor del artículo "una vez que se han instalado en el ordenador del usuario y han aprendido lo que querían saber, hacen lo mismo que el extraterrestre de Steven Spielberg: llamar a casa para contarlo". Aparte del tono humorístico de la definición, la verdad es representa una imagen muy nítida de qué es exctamente el *spyware*.

Por último y en relación con el adware, debemos referirnos a una modalidad especial del mismo que es el denominado "*improve your experiencie software*", o software de mejora de experiencia. En él, se informa al usuario de que si consiente, serán recabados datos de navegación y otros (no especifica normalmente), a fin de "hacer más agradable su experiencia con nuestros productos" [(41)]. Ocultando la verdadera finalidad de los mismos que no es otra que establecer perfiles de usuarios. Nuevamente aquí entraríamos en la vulneración de los art.4, 5,6 y 11 de la LOPD, que tantas veces hemos citado ya.

3.2. Aspectos jurídicos.

El *spyware* es capaz de recoger todo tipo de informaciones (programas instalados, documentos existentes, correos electrónicos, contraseñas, etc.). Es por ello que en este punto debemos hacer una remisión general a lo dicho para el adware, a fin de no repetir la explicación. (vulneración de los principios de finalidad, congruencia, proporcionalidad, información, lealtad, etc.)

Sin embargo vamos a realizar aquí un breve estudio de **Derecho comparado** a fin de ver como se podría regular el fenómeno del *spyware* con base de la experiencia de otros países.

Como dijimos en el caso del *adware*, la regulación actual en Europa frente a estos nuevos métodos de vulneración de la privacidad es prácticamente inexistente (a excepción de los Considerandos de la Directiva 2002/58/CE y de las propuestas del Grupo de trabajo sobre protección de datos del art.29, que no tienen fuerza normativa en sí). En este sentido, otros países, especialmente EE.UU, están mucho más avanzados en cuanto a regulación y positivación de estas nuevas prácticas. De hecho, y en relación con el *spyware* (incluyendo aquí el adware), cabe destacar la "*spyware* Control and Privacy Proteccion Act de 2001", que suponen un primer intento de legislar sobre estos nuevos peligros desconocidos hasta el momento.

La *spyware* Control and Privacy Protection Act of 2001, viene a establecer en su sección 2.(a) (2) el requisito del *consentimiento expreso*. Se establece a través de dicho artículo que no se podrá coleccionar información sobre el *software* o *hardware* instalado en la computadora del usuario, o la manera en que ésta es usada, con independencia de si se trata de un programa gratuito o no "unless the user of such computer software provides

[41] MSN Messenger de Microsoft, entre otros.

affirmative consent" [42]. Como vemos, el legislador estadounidense a tomado en este sentido el mismo camino que el comunitario en el supuesto del *spam*, mediante la Directiva 2002/58/CE.

Asimismo, la sección 2.(a) (1), establece tres **requisitos referidos a la información** que ha de proporcionarsele al usuario del programa antes de la instalación del mismo. De esta manera se estaría desvirtuando la concepción tradicional de *spyware*, cuya propia denominación hace referencia a lo oculto del sistema de tratamiento ("espía"). Los requisitos establecidos son:

a) "*Información clara y visible*, en la primera página electrónica de las instrucciones de instalación". A través de este requisito estaríamos tratando de poner solución al problema de la oscuridad e ilegibilidad de las licencias de uso.

b) Información sobre *qué datos van a ser recogidos*, así como de la *identidad* (nombre y dirección) *del responsable* del tratamiento y de aquéllos a quienes se vayan a ceder los datos.

c) Se debe *posibilitar al usuario que deshabilite la función de recogida de datos*, "sin afectar, por lo demás al funcionamiento del software".

Como podemos observar, estos requisitos son semejantes a los principios establecidos a nivel europeo en cuanto a la recogida y tratamiento de datos de carácter personal. El primero podría vincularse al principio de información del art.5 LOPD, estableciendo al igual que este, criterios de claridad en la prestación de la información. El segundo requisito sería equiparable al art.20 LSSI en materia de comunicaciones comerciales vía e-mail. En tanto que el tercero de los requisitos sería asimilable al derecho de oposición recogido por el legislador español en los arts.6.3 y 6.4 LOPD.

En cuanto a los **derechos de los interesados**, la sección 2.(a) (5) establece los siguientes:

a) Derecho de acceso a la información recolectada.

b) Derecho a corregir, borrar o añadir información.

En este caso, el legislador no prevé un registro, ni las particularidades por las que se puede llevar a cabo cada una de las acciones previstas, sin embargo los derechos aquí vienen nuevamente a ser similares a los establecidos por el legislador interno.

Del mismo modo, la sección 2.(a) (6) establece el principio de seguridad de los datos, al igual que lo hace el art.9 LOPD.

[42] Sin que el usuario del software otorgue afirmativamente su consentimiento

Por último señalar que la "Spyware Act" establece una serie de excepciones al derecho de información y consentimiento, que en este caso, sí difieren de lo que nosotros conocemos. La sección 2.(a) (3) establece tres excepciones, a las que hay que sumar las de la sección 2.(d) (1):

• Los casos en que sea necesaria su utilización a fin de comprobar si el programa utilizado no es una copia o una distribución ilegal del mismo, contribuyendo así a la protección de la propiedad intelectual del software.

• Proveer, previo requerimiento del usuario, soporte técnico. En este caso, a nuestro modo de ver, la norma se está refiriendo a aquellos casos en los que, como ocurre con los antivirus, es necesaria una actualización periódica, que sucede muchas veces sin el conocimiento del usuario y para lo cual se necesitan ciertos datos del registro del sistema, así como la dirección IP entre otros.

• Los casos en los que en una relación laboral, el patrón hace uso de *spyware* a fin de controlar la actividad de los empleados.

• Los casos en los que es necesario el empleo de *spyware* para obtener información en sede de procedimientos civiles o penales, cuando no sea posible obtenerla de otro modo en el caso de los primeros.

Como vemos, no existe tanta diferencia entre el régimen general interno de protección de datos y la normativa específica estadounidense en materia de *spyware*. Y es que si los derechos a proteger son prácticamente los mismos, y la amenaza es tan técnica, es lógico que, de acuerdo a la tecnología actual disponible, los medios para hacer frente a estas nuevas formas de intrusión, no difieran mucho de unos países a otros.

X. COOKIES (GALLETAS O CHIVATOS)

1. ¿Qué son?

Las *cookies* son pequeños archivos de texto, en formato *ASCII*, que determinados servidores envían al ordenador del usuario durante la navegación al acceder a ellos. Dado que se trata de archivos de texto, como cualquier otro archivo, su comunicación a través de Internet depende del protocolo TCP/IP. El problema reside en el hecho que el protocolo HTML también permite su envío a través del charloteo del navegador ya estudiado, mediante la instrucción SET-COOKIE. Como ocurre con el resto de datos transmitidos por el charloteo del navegador, el usuario que en ese momento esta accediendo al servidor no conoce a ciencia cierta que está ocurriendo. Sin embargo, es una peculiaridad de las *cookies* el hecho de que puedan almacenarse en disco duro del ordenador del usuario (y no tan sólo en la memoria RAM o en la caché), sin que este tenga, como en la mayoría de casos, conocimiento.

Una vez que una *cookie* se almacena en el disco duro del usuario, el servidor, en las posteriores ocasiones que se acceda al mismo desde ese ordenador (y siempre que no se haya eliminado de algún modo la *cookie*), identificará el usuario y será capaz de leer la información almacenada en el archivo de texto del disco duro de la computadora, a través del campo COOKIE en el charloteo del navegador. Esto, lógicamente, puede conllevar serios peligros para la privacidad dependiendo de cual sea la información que se almacene en la *cookie*.

Un ejemplo práctico servirá para hacernos a una idea de cómo es una *cookie*:

• consumo@warnerbross[1].txt: éste es el nombre de la *cookie* en nuestro disco duro. En cuanto al contenido es el siguiente:

WBWTID

62.82.236.237-3FA989A13BC000000720863-whatisthematrix-janus

warnerbros.com/

1536

4053983232

30051033

1594679136

29598709

*

De todo el contenido de la *cookie*, y sin grandes conocimientos de informática sólo podemos averiguar la dirección IP enviada por la *cookie*. En este caso se trata del servidor que aloja la página www.whatisthematrix.com, con dirección IP 62.82.236.237. El resto de datos y números no podemos saber que significan, y, aún más, no sabemos que finalidad tienen. Sin embargo, aquél de quién procede el envío de la *cookie* es perfectamente capaz de leerlas e interpretarlas.

Entre la información que puede contener una *cookie* [43] encontramos:

-páginas visitadas hasta el momento

-anuncios consultados

-número de identificación del usuario -global único-

[43] Documento de trabajo: *Privacidad en internet: enfoque comunitario integrado de la protección de datos en línea*, aprobado por el Grupo de Trabajo sobre protección de datos del artículo 29, el 21 de noviembre de 2000, WP 37, 5063/00/ES/final

-etc.

En cuanto a los tipos, podemos diferenciar entre *cookies permanentes* y *cookies de sesión*, en atención al tiempo en que residen en el disco duro del usuario. Las primeras continúan activas en el ordenador del mismo durante el tiempo predeterminado por las mismas a la hora de ser creadas, incluso después de ser apagado el mismo. Su plazo de *expiración* puede ir desde una pocas horas hasta años.

En cambio, las denominadas *cookies* de sesión expiran una vez a finalizado la conexión.

2. Riesgos reales para la privacidad.

Se ha especulado mucho acerca de lo que son capaces de hacer las *cookies*, sin embargo la respuesta es sencilla. Las *cookies* son **archivos de texto plano**. Ello supone que sólamente pueden leerse desde el servidor o sitio web que fueron enviadas [(44)], pero que, **en ningún caso podrán alterar elemento alguno del ordenador, pues *no* son archivos ejecutables**.

Las *cookies* fueron creadas en un principio en beneficio del usuario. A través de ellas se trataba de personalizar las páginas web en cuanto a diseño, evitar que el usuario se registrara cada vez que quisiera acceder a determinados contenidos de una página, etc. En la actualidad, dentro de estas funciones, destaca la de los llamados *carritos de compra*. Esto es, cuando una persona accede a una página de venta on-line, probablemente no sea la única que esté en ese momento navegando por dicha página. Si ambas quisieran comprar un producto a la vez, el servidor, y por tanto, la empresa, tendría problemas a la hora de identificar cuál de los usuarios que está navegando en ella es el comprador. Las soluciones a este problema (posibilitar sólo un acceso simultáneo, registros del usuario a cada momento, etc.) conllevarían en muchas ocasiones atrofia en el tráfico. Para ello, lo que se hace es instalar en el ordenador del futuro comprador una *cookie* con un número de identificación único, para así saber en cada momento quién está actuando en la operación de compraventa y posibilitarle el pago del conjunto adquirido al final de la navegación.

Sin embargo, en otras oacasiones este instrumento no es utilizado con fines tan legítimos. A través de las *cookies* técnicamente no es posible averiguar datos sobre el ordenador donde residen, tales como programas instalados, direcciones de correo electrónico de la agenda de direcciones u otros. El único dato de carácter personal del usuario que se puede conocer a través de las *cookies* es sus *hábitos de navegación*. Hemos de partir, como ya hemos dicho, de que las *cookies* sólo pueden ser leídas por el sujeto responsable del envío a través de la página web o servidor del que fueron enviadas. El problema reside en aquellos supuestos en los que el responsable "participa" en páginas web de diversa índole a través de hipervínculos invisibles. En estos casos, cuando una *cookie* ha

[44] Si bien es cierto que se conocen varios agujeros de seguridad, especialmente en Internet Explorer, que permiten leer el directorio c://windows/*cookies* desde cualquier página web

sido instalada en el ordenador del usuario y éste accede a otra página donde el servidor web que la envió posee otro hipervínculo invisible, lo que sucederá es que el responsable de la *cookie* será capaz de conocer diversos datos, en distintos momentos, que le ayuden a elaborar un perfil del usuario en cuanto a sus hábitos de navegación.

Como dijimos, mediante el uso de las *cookies* se puede conocer la página anterior a la visitada, la hora de acceso a ésta última y el tiempo de permanencia entre otros. Si a ello le sumamos el conocimiento por el mismo responsable de la página que fue visitada en un momento posterior dentro de la misma sesión de navegación, o en otra, junto con la hora y tiempo de duración, la temática de las páginas visitadas, y el hecho de que haya visitado algún *banner* o no, arroja como vemos mucha información a fin de reconstruir un perfil del sujeto. La pregunta sería en este caso si los hábitos de navegación son un dato de carácter personal o no.

El art.2 LOPD define datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". Como vimos en su momento [(45)], los requisitos para saber si un dato era o no de carácter personal eran 1) que se tratara de un dato concerniente a una persona física (cualquier dato bastaría); y 2) que esa persona fuera identificable de acuerdo a actuaciones razonables.

En relación con el primero de los presupuestos podemos señalar que los hábitos de navegación son, desde luego, datos concernientes a las personas físicas, en el sentido de que permiten conocer aspectos tales como sus gustos, aficiones, el ámbito laboral en que se desenvuelven o, incluso datos especialmente sensibles, tales como comportamientos sexuales (imaginémonos el acceso a determinadas páginas de contenido erótico o pornográfico, o a tiendas que vendan productos de este tipo); afiliación sindical o tendencias políticas (páginas web de partidos políticos o asociaciones sindicales o afines) o religión, entre otros.

Comprobado el hecho de que los hábitos de navegación son datos concernientes a una persona física, habremos de establecer si estos datos permiten identificarla de acuerdo a parámetros razonables.

Como ya hemos dicho, cada *cookie* es única e independiente del resto gracias a un número de identificación. Al almacenarse en el disco duro la *cookie*, se está almacenando también el número que permite identificarla. Lo que ocurre, como vemos, es que, si bien de modo directo no estamos identificando al usuario, de modo indirecto sí que estamos vinculando un ordenador a un número a través de la *cookie* en él instalada. Esto, en el supuesto de ordenadores personales, y unido a otros factores, tales como el conocimiento de la IP (especialmente en aquellos supuestos en que nos encontremos ante IPs estáticas), puede llegar a suponer una grave vulneración de la privacidad y del derecho a la autodeterminación informativa. Pensemos por un momento de manera excesiva e imaginémonos que no se nos permite acceder a una página con un contenido concreto (por ejemplo a una página de derechos humanos), porque en un momento anterior de la

[45] Ver apartado "Dato de carácter personal: concepto"

navegación, hemos visitado otra página de contenido antagónico (por ejemplo una página de apología de la violencia con objeto de realizar un trabajo). Esto, que en principio puede parecer un ejemplo muy simple, se puede convertir en un verdadero problema si por ejemplo la página visitada era sobre una asociación de ayuda a afectados del cáncer, y la empresa responsable de la *cookie* es una aseguradora...

3. Regulación existente. Especial atención al Considerando 25 de la direcitva 2002/58/CE.

En el panorama nacional y europeo no existe ninguna norma que haya regulado el fenómeno de las *cookies* de manera específica, ni tan siquiera en el ámbito de otra norma de carácter general. Esto supone desde luego un vacío legislativo que deberá de solventarse de algún modo, pues la realidad extrajurídica está ahí.

Dado que las *cookies* pueden atentar contra la privacidad de las personas, habremos de aplicar la normativa relativa a la protección de datos de carácter personal, que en este caso estará representada por la Ley 15/1999 de Protección de datos de carácter personal, y por la Directiva 2002/58/CE, en el sentido en que le es aplicable de acuerdo con lo señalado en el apartado referente a la normativa aplicable en el tratamiento invisible de datos personales

En relación con la LOPD, la utilización de las *cookies*, sin puesta en conocimiento previo del usuario estaría vulnerando tres aspectos fundamentales: el derecho a la información (art.5), el principio de consentimiento (art.6), y el principio de lealtad (art.4.7). Además, en los casos en los que se utilice la *cookie* para fines distintos de los señalados, se estaría violando también el principio de congruencia del art.4.2.

En relación con el *derecho de información* del usuario, parece claro que si la *cookie* se almacena en el ordenador del mismo sin aviso previo, se está vulnerando claramente. Pero no sólo se estaría vulnerando con ello el derecho a la información, sino también el *principio de lealtad*, por cuanto supone una manera de recogida de datos desleal o fraudulenta, y el de *prestación del consentimiento*, en tanto no se otorgue al usuario la posibilidad de optar porque ese archivo de texto, no siendo necesario para la navegación en sí (*principio de proporcionalidad*), no se grabe en el disco duro del ordenador referido.

Los navegadores, por lo general, ofrecen opciones de privacidad donde el usuario puede configurar las preferencias acerca de la información y aceptación de *cookies*. Mediante estas opciones se puede establecer que se avise cada vez que una *cookie* sea enviada al navegador, que se avise sólo en determinados supuestos, o que no se avise nunca. Del mismo modo se puede señalar que dichas *cookies* sean aceptadas siempre, sólo cuando provengan de determinados servidores, o nunca. Sin embargo, estas posibilidades que ofrecen los *browser* no eximen al responsable de las *cookies* de cumplir con todos los deberes que la ley establece (informar, pedir el consentimiento, etc.), sino que son simples medidas a favor de la privacidad que los diseñadores de navegadores han incluído, ante la total falta de actuación por parte de los responsables en este sentido.

Asimismo, puede ocurrir que previamente al envío de una *cookie*, se informe al usuario de cuál es la finalidad de la misma de una manera clara y precisa, y se pida su consentimiento para el envío o no. Se estaría también vulnerando la normativa sobre protección de datos, lógicamente, si no hubiera congruencia entre la finalidad para la que se prestó el consentimiento, y la verdadera finalidad de la *cookie*. Es decir, si por ejemplo se señalase que la *cookie* tiene como función personalizar la pantalla de bienvenida a una página web de acuerdo a los gustos del usuario, pero posteriormente se utilizara para comprobar los hábitos de navegación.

Respecto de la aplicación de la Directiva 2002/58/CE, el artículo más significativo que resulta de aplicación es el quinto, referido a la confidencialidad de las comunicaciones y datos de tráfico. En este sentido, y al igual que en el caso de los *web bugs*, la Directiva impone un mandato a los estados miembros de garantizar la confidencialidad de las comunicaciones, ocultando los datos de tráfico y la identificación de llamada, entre otros (Considerando 15 y artículos 5 y 8 de la Directiva). Sin embargo, y a diferencia de en el caso de los *web bugs*, la confidencialidad de la IP no supone una cesación indirecta del uso de las *cookies*, por cuanto éstas, para identificar al usuario, no se basan en la IP del ordenador del mismo, sino un identificador único que, a diferencia de la IP (en el caso de ser ésta dinámica), siempre será el mismo.

Ahora bien, en relación con la Directiva 2002/58/CE, es especialmente significativa la inclusión del extenso Considerando 25. En él se dice lo siguiente: "No obstante, los dispositivos de este tipo, por ejemplo los denominados "chivatos" (*cookies*), pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo para analizar la efectividad del diseño y de la publicidad de un sitio web y para verificar la identidad de usuarios partícipes en una transacción en línea. En los casos en que estos dispositivios, por ejemplo los denominados "chivatos" (*cookies*), tengan un propósito legítimo, como el de facilitar el suministro de servicios de la sociedad de la información, debe autorizarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un "chivato" (*cookie*) o dispositivo semejante. Esto es particularmente importante cuando otros usuarios distintos al usuario original tienen acceso al equipo terminal y, a través de éste, a cualquier dato sensible de carácter privado almacenado en dicho equipo. La información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores. La presentación de la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un "chivato" (*cookie*) o dispositivo similar, en caso de que éste tenga un propósito legítimo".

Como vemos, el legislador comunitario ha desarrollado en este Considerando una serie de previsiones muy concretas acerca de la regulación de las *cookies*. Sin embargo, es

ciertamente sorprendente, que, al igual que en el caso del Considerando 24 respecto al *spyware* y los *web bugs*, esto no tenga reflejo en el articulado. Pareciera como si el legislador no se hubiera atrevido a regularlo definitivamente. Y es que el problema radica en que, como por todos es bien sabido, los Considerando en sí no tienen valor normativo, les sucede como a los preámbulos de muchas leyes internas. En todo caso podría atribuírsele cierto valor interpretativo. Ahora bien, en aquellos supuestos en los que se infrinja el Considerando, por ejemplo supeditando el acceso a una página web a la aceptación de una *cookie*, con fines no legítimos o desconocidos, muy probablemente el aplicador interno optará en buena medida por aplicar la normativa interna y prescindir de la voluntad del legislador comunitario. Y la resolución de si estará o no actuando correctamente es algo que en este momento no podemos apreciar, pues sólo será posible en el momento en que alguien interponga un recurso por omisión frente al Estado incumplidor, y el TJCE se pronuncie en el caso concreto.

En resumen. De acuerdo con la normativa sobre protección de datos, el uso de las *cookies* estará permitido *siempre* que:

•Se informe al usuario de su envío.

•Se informe al usuario de la finalidad expresa de las mismas.

•Se posibilite la prestación o no del consentimiento.

•Se cumplan el resto de principios derechos establecidos por la LOPD (lealtad, congruencia, proporcionalidad, derecho a oposición en un momento posterior, etc).

•Además, de acuerdo con lo dispuesto en el artículo 26 LOPD, debería notificarse a la Agencia de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

BIBLIOGRAFÍA

DAVARA RODRÍGUEZ, M. A, *Manual de Derecho*, 5ª. Ed., Aranzadi, Pamplona, 2003.

DE ASÍS ROIG, A.E., "Protección de datos y derecho de las telecomunicaciones", en CREMADES. J., FERNÁNDEZ-ORDÓÑEZ, M.A., e ILLESCAS, R. (coords.), *Régimen Jurídico de i*nternet, La ley, Madrid, 2001.

DE MIGUEL ASENSIO, P.A., *Derecho privado de Internet*, 3ª. Ed., Cívitas, Madrid, 2003.

DEL PESO NAVARRO, E., *Ley de Protección de Datos: la nueva LORTAD*, Madrid, 2000.

EGUSQUIZA BALSAMEDA, M.A., "Intimidad del consumidor y protección de datos", MORO ALMARAZ, M.J. (dir.), *Internet y Comercio Electrónico*, Aquilafuente, Salamanca, 2003.

GÓMEZ MULAS, V., *La nueva Ley de Internet*, La Ley, Madrid, 2003.

GRINGRAS, C., *Laws of Internet*, 2ª. Ed., Butterworth, Londres, 2003.

HERRÁN ORTÍZ, A. I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dyckinson, Madrid, 2002.

HERRERA BRAVO, R. "Privacidad en Internet: el problema del tratamiento invisible y automatizado de datos personales", en DAVARA RODRÍGUEZ, M.A. (coord.), *XVIII encuentros sobre informática y derecho*, Universidad Pontifica Comillas, Madrid, 2003.

MARROIG POL, L. Y CORRIPIO GIL-DELGADO, M., "El ordenamiento español y la protección de datos personales en el sector de las telecomunicaciones", en *Boletín de información del Ministerio de Justicia,* 2002, nº 2.

RIBAS, J. "Riesgos legales en Internet. Especial referencia a la protección de datos personales", en "REDDETI: Revista de derecho de las telecomunicaciones e infraestructuras en red", número 3, 2000.

ROCAS JUNYENT, M. Y TORRALBA MEDIOLA, E. "Derecho a la intimidad: el secreto de las comunicaciones e Internet", en CREMADES J., FERNÁNDEZ-ORDÓÑEZ, M. A. E ILLESCAS. R. (coords.), *Régimen Jurídico de Int*ernet, La Ley, Madrid, 2001.

SUÑÁS LLINÁS, E., *Tratado de Derecho informático*, Universidad Complutense, Madrid, 2002.

VÁZQUEZ IRUZBIETA, C., *Manual de Derecho informático*, Dijusa, Madrid, 2002.

VEN SANTOS, J. M., "Derechos fundamentales, Internet y nuevas tecnologías de la información y la comunicación", en GARCÍA MEXÍA, P. (dir.), *Principios de Derecho de Internet*, Tirant Lo Blanch, Valencia, 2002.

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

JURISPRUDENCIA

-Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre.

-Sentencia Tribunal Constitucional 202/1999, de 8 de noviembre.

-Sentencia Audiencia Nacional, de 21 de noviembre de 2002. (RJCA 2003\40).

-Sentencia Audiencia Nacional, de 15 de noviembre de 2002 (RJCA 2003\14).

-Sentencia Audiencia Nacional, de 8 de noviembre de 2002. (RJCA 2003\8).

-Sentencia Audiencia Nacional, de 7 de noviembre de 2002. (RJCA 2003\7).

-Sentencia Audiencia Nacional, de 15 de marzo de 2002. (RJCA 2002\784).

-Sentencia Audiencia Nacional, de 28 de septiembre de 2001. (RJCA 2002\272).

-Sentencia Audiencia Nacional, de 14 de septiembre de 2001. (RJCA 2002\271).

-Sentencia Audiencia Nacional, de 7 de julio de 2001. (RJCA 2001\73).

-Sentencia Audiencia Nacional, de 25 de enero de 2001. (RJCA 2001\831).

-Sentencia Audiencia Nacional, de 12 de enero de 2001. (RJCA 2001\865).

-Sentencia Tribunal Superior de Justicia de Cantabria, de 10 de enero de 2003. (RJCA 2003\5).

-Sentencia Tribunal Superior de Justicia de Extremadura, de 25 de noviembre de 2002. (RJCA 2002\1184)

-Sentencia Tribunal Superior de Justicia de Cataluña, de 31 de julio de 2001. (RJCA 2001\1467).

-Sentencia Tribunal Superior de Justicia de Madrid, de 15 de febrero de 2001. (RJCA 2001\948).

-Sentencia Tribunal Superior de Justicia de Madrid, de 7 de febrero de 2001. (RJCA 2001\699).