E.M. nº 38 Mayo-Agosto 2011

LIBERTAD COMERCIAL Y PRIVACIDAD JURÍDICA: UN DIFÍCIL EQUILIBRIO EN LA RED

David López Jiménez
Universidad de Sevilla

1. INTRODUCCIÓN

Internet ha establecido, cuantitativa y cualitativamente, uno de los mercados más colosales del planeta. En efecto, la red de redes no ostenta la mencionada cualidad, solo por el ingente volumen de personas que diariamente hacen uso de la misma –que, dicho sea de paso, es de carácter creciente-, sino también por la enorme variedad de usuarios, procedentes de múltiples lugares geográficos y con diversos niveles de poder adquisitivo. Aunque los usuarios de Internet pueden, *a priori*, recurrir al mismo con numerosas finalidades, que, naturalmente, podrán ser extraordinariamente diversas entre sí, lo cierto es que todos ellos, en mayor o menor medida, visionarán, tarde o temprano, algún anuncio publicitario difundido en tal canal.

La publicidad en línea es una fuente esencial de ingresos para un elevado abanico de servicios en la Red, siendo, además, un factor importante en el crecimiento y la expansión de la economía de Internet. La tecnología básica de este último, como veremos en el siguiente estudio, permite a los proveedores de publicidad en red rastrear, de manera continuada, datos personales de determinados usuarios en distintos sitios de Internet. En otros términos, la publicidad basada en la navegación efectuada en Internet implica, en virtud de ciertas técnicas electrónicas que en ocasiones pueden ser plenamente invisibles, la identificación de los usuarios que navegan por la Red y la creación gradual de perfiles que después servirán para enviarles publicidad de acuerdo con sus intereses.

Son realmente importantes los beneficios económicos que la publicidad basada en el comportamiento en la Red pueda aportar a la propia industria, que se sirve de la misma, pero esta práctica no debe, en ningún caso, realizarse a expensas de la protección de datos de carácter personal de los usuarios.

De acuerdo con la relevancia que, en la práctica, supone la publicidad basada en el comportamiento, los requisitos de transparencia son una condición fundamental para que los usuarios consientan la recogida y el tratamiento de sus datos personales y ejerzan sus opciones. Como veremos en el presente trabajo, existen ciertas obligaciones de información que los proveedores de redes de publicidad deberán cumplir respecto de las personas afectadas.

Aunque la legislación sobre protección de datos exige, entre otras cosas, que para realizar esta práctica se recabe el consentimiento informado de las personas, es bastante dudoso que el usuario medio sea consciente y, menos aun, consienta ser controlado para recibir publicidad a medida. Por ello, un complemento idóneo, como advertiremos, pasa por incentivar el fenómeno de la autorregulación de la industria.

En definitiva, como en el presente estudio veremos, la privacidad debe gozar de un nivel de protección relativamente alto, pues no es, en absoluto, una cuestión baladí. Constituye un aspecto sumamente importante que ha de ser necesariamente respetado, ofreciendo a los propios usuarios la opción de decidir si deciden otorgar su consentimiento a efectos de que su comportamiento pueda ser rastreado con fines publicitarios.

2. DIVERSIDAD DE TÉCNICAS SUSCEPTIBLES DE ELABORAR PERFILES DE LOS USUARIOS

Los datos de carácter personal, en la actualidad, tienen un extraordinario valor (Muñiz Casanova y Ariz López de Castro, 2004). En este sentido, los perfiles constituidos se compran y se venden a un precio nada desdeñable (D´Orazio, 1999) y, lo peor de todo, se trata de una actividad invasiva de nuestra intimidad (Ngai y Wat, 2001; Bigné Alcaniz, Ruiz Mafé y Andreu Simó, 2005; Sharma y Shet, 2004), pues, en muchas ocasiones, no habrá resultado, en absoluto, conocida ni, mucho menos, consentida (Juliá Barceló, 2000; Serra Rodríguez, 2000; Llácer Matacás, 2003; Jawahitha, 2004).

De hecho, existen numerosos mecanismos tecnológicos ideados para tal fin (Bensoussan, 1998; Schwartz, 2004; Martínez Martínez, Fernández Rodríguez y Saco Vázquez, 2008) cuáles, entre otros, son, las *cookies*, troyanos, *spyware* y *web bugs*. Estas aplicaciones y otras similares pretenden monitorizar nuestro comportamiento en la Red. Obviamente, cuanto mayor sea el tiempo que estemos conectados, más elevado será el volumen de información de carácter personal que tales instrumentos recopilen. Las conexiones dejan huella que, junto los datos obtenidos por tales técnicas, pueden llegar a identificarnos, vulnerando, de este modo, nuestra privacidad. No debe pasarse por alto que no resulta necesario celebrar electrónicamente un contrato para que se aporten datos personales. Simplemente es suficiente con comenzar a navegar por Internet para que, de forma tanto consciente como, en muchos casos, inconsciente, se aporten datos personales (Rico Carrillo, 2003; Guillén Catalán, 2005; Madrid Parra, 2008).

Sería ingenuo manifestar que el único móvil que puede tener el recurso a estas técnicas es exclusivamente de índole comercial, ya que, entre otros fines, pueden utilizarse para controlar a los trabajadores, o fines de seguridad nacional, si bien nos centraremos en aquél aspecto por ser el que más interesa a efectos del presente trabajo. Así, respecto a la defensa nacional, por ejemplo, a finales de 2001, en el seno del proyecto *Cyber Knight*, el FBI creó un virus, denominado *Magic Lantern*, para instalarlo en los ordenadores de presuntos sospechosos y, de este modo, obtener sus claves criptográficas. El virus se envía al ordenador del sospechoso bien a través del correo electrónico bien aprovechando las eventuales vulnerabilidades de seguridad del propio sistema operativo o de ciertos programas. Es oportuno destacar que la forma de recabar las claves pasa por la instalación de un *key logging* que registrará las pulsaciones del teclado (Nabbali y Perry, 2003; Kussmaul, 2007; Golumbic, 2008; Janczewski y Colarik, 2008).

El potencial de esta información es enorme (Ribas Alejandro, 1999; Grimalt Servera, 2004; Payeras Capellá, 2005), desde la perspectiva del marketing, pues con la misma se podrán ofrecer productos o servicios adicionales, sean propios –venta cruzada- o de terceros –productos complementarios- remitir correos electrónicos, lo más personalizados posibles sobre bienes y/o servicios que pudieran, o debieran, interesar a su destinatario, redireccionamiento de la publicidad o *retargeting* -dirigido a los usuarios que visitaron una tienda virtual (pero que no compraron nada), animándoles a regresar por medio de publicidad segmentada en los sitios *Web* que visiten posteriormente-, etc. (Wenz, 2001; Baskin y Piltzecker, 2006; Treese y Stewart, 2003; Gutiérrez González, Pedreira Sánchez y Velo Miranda, 2005; Croll y Power, 2009; Levine y Levine, 2010). En definitiva, un elenco de posibilidades realmente amplio para los prestadores de servicios que enlazan con la denominada publicidad comportamental.

Las *cookies* son pequeños ficheros de texto, que algunos servidores *Web* piden a nuestro navegador -Internet Explorer, Firefox, Opera, Safari, Chrome, etc.-, que escriben en nuestro disco duro información sobre lo que hemos estado haciendo en sus páginas (Palmer, 2005; Erdozáin López, 2007). La *cookie* está formada por el nombre del usuario configurado en el navegador, seguido del símbolo arroba (@), y el nombre del servidor que envía la *cookie*, más la extensión "txt" que la

identifica como fichero de texto (Fernández Rodríguez, 2004). El potencial de esta información, a efectos de marketing, es enorme (Grimalt Servera, 2004; Payeras Capellá, 2005).

Las *cookies* pueden clasificarse en función de dos criterios. En primer término, en atención a su duración, puede distinguirse entre *cookies* de sesión o temporales –sólo se requieren mientras se mantiene la sesión del usuario y al finalizar ésta desaparecen- y permanentes o definitivas –subsisten en el ordenador tras la finalización de la conexión pudiendo ser recuperadas por el servidor en posteriores sesiones-. Los objetivos de ambas modalidades son, entre otras, ahorrar tiempo al usuario –al identificarle como miembro, y, de este modo, no tener que pedirle en cada ocasión que introduzca la identificación del usuario y la contraseña- y ofrecerle información personalizada. En segundo lugar, desde el punto de vista de su procedencia, podemos hablar de *cookies* de primeros –las originan el propio sitio *Web* que se está visitando- y *cookies* de terceros –procede de un sitio *Web* diferente, generalmente se colocan por empresas de publicidad en Internet-.

Una modalidad de *cookies* particularmente espinosa, por los efectos vulneradores de la privacidad, son las *cookies* basadas en la tecnología *fash* –llamadas también *supercookies*-. A título anecdótico, diremos que pueden almacenar veinticinco veces más de contenido que una *cookie* de rastreo tradicional y comparten información entre diferentes navegadores, ya que no las gestionan estos últimos, sino el *plugin* de *flash*. Se trata de *cookies* relativamente desconocidas para los propios navegadores, dado que, como regla general, no se pueden controlar a través de la configuración de privacidad del navegador. En otras palabras, no son las *cookies* que podríamos calificar de tradicionales, a las que, dicho sea de paso, ya nos hemos referido, sino que sólo trabajan en *flash*. De esta manera, volviendo a insistir en lo que hemos adelantado, aunque el usuario tenga preconfigurado el navegador, en modo de navegación segura, no es óbice para que las *cookies flash* realicen la labor para la que han sido concebidas. Aunque la finalidad de esta tipología de *cookies* parece ser la misma que las que ostentan carácter tradicional -publicidad basada en el comportamiento o publicidad comportamental-, son, si cabe, más invasivas de la privacidad, dado que, entre otras actuaciones, pueden recuperar *cookies* de rastreo tradicionales borradas o rechazadas previamente por el usuario. Esta última práctica se conoce como *respawning*.

En cuanto a los troyanos (como los *trap doors* o puertas falsas –que consisten en la introducción en los sistemas informáticos a través de accesos o puertas de entrada no previstas en las instrucciones de aplicación de los programas-, *logic bombs* o bombas lógicas -únicamente se activan bajo ciertas condiciones, entre otras, en una determinada fecha, la existencia de un fichero con un nombre, o el alcance de un número de ejecuciones del programa que contiene la bomba -y *data diddling* o *tampering* o modificación de datos- que se refiere a la alteración desautorizada a los datos o del *software* del sistema, incluyendo borrado de archivos-), cabe decir que son instrumentos que establecen, de forma automática y oculta para el afectado, determinadas instrucciones en los programas instalados en el ordenador para, de este modo, lograr cierta información del usuario (Piqueres Castellote, 2006).

Los *spyware* son programas espía que monitorizan el comportamiento de los consumidores y, adicionalmente, ocasionan fallos en el rendimiento y estabilidad de los ordenadores (Klang, 2003; Schultz, 2003; Bruening y Steffen, 2004; Radcliff, 2004; Stafford y Urbaczewski, 2004; Urbach y Kibel, 2004; Volkmer, 2004; Sipior, Ward y Roselli, 2005). Podemos diferenciar tres grandes tipos de *spyware*: 1) El *snoopware*, que son los *keystroke loggers* –lectores de las pulsaciones del teclado- y las utilidades de captura de pantalla; 2) El *adware* y aplicaciones similares empleadas para seguir el comportamiento del usuario y aprovechar su conexión a Internet; 3) Los identificadores únicos de los programas o del *hardware*, campo en el que es habitual referirse a los espías de *Microsoft* e *Intel*.

Debe, además, subrayarse que los *spyware* rastrean información sobre hábitos de consumo y navegación sin que el usuario lo sepa y, normalmente, se conectan a un servidor de la compañía que los distribuyó para transmitírsela. Asimismo, procede destacar que comienzan a funcionar solos, sin

conocimiento ni consentimiento del usuario, hacen un uso no autorizado del ordenador y transmiten información personal (Fernández Teruelo, 2007).

Respecto a los *web bugs*, también denominados bichos o escuchas en la Red, "píxeles transparentes", "*web beacons*", "*pixel gif*" o "*web pings*", tienen que ver con actuaciones inconscientes cuya repercusión podría pasar desapercibidas (Martín, Wu y Alsaid, 2003). En efecto, para registrar y rastrear la apertura de un documento -por ejemplo, un correo electrónico- por Internet, se incluye en el mismo una imagen vinculada a un servidor distinto al que aloja la página *Web* que estamos visitando (Bennett, 2001). Son gráficos, de un píxel por un píxel, que instalan un programa en el disco duro con la finalidad de leer todas las *cookies* incluidas en el mismo (Harding, Reed y Gray, 2001). Cuando se abra la página *Web* se pedirá al servidor ese archivo y quedará registrada la IP -*Internet Protocol*- del solicitante. El hecho de solicitar la imagen vinculada permitirá recabar, entre otras cuestiones, la dirección IP del ordenador, la fecha y hora en que se visitó la página *Web* donde estaba insertada la imagen, el tipo y versión de navegador del consumidor o usuario, su sistema operativo, el idioma predeterminado o los valores de *cookies*. De esta manera, se recogen numerosos datos estadísticos y se consigue efectuar el seguimiento de los usuarios (Payeras Capella y Ferrer Gomilla, 2004).

Los *mail bugs* son los *bugs* que se incorporan en los mensajes de correo. Cuando se procede a la visualización del mensaje de correo electrónico, la imagen se descargará del servidor. Al ser incorporadas a los mensajes de correo electrónico, enviarán información que revelarán que el mensaje que lo contiene ha sido abierto, verificando, de este modo, que la dirección receptora es real. Una vez realizada esta comprobación, esta dirección podrá ser utilizada para el envío de correos electrónicos no solicitados -*spam*-. Si el *mail bug* contiene un identificador único podría ser empleado para determinar si un mensaje es enviado.

3. OBSERVANCIA DE CIERTAS CAUTELAS PARA GARANTIZAR EL RESPETO DE LA PRIVACIDAD

Impedir el uso de los dispositivos enunciados o, al menos, que se haga dentro de ciertos límites que garanticen, en todo caso, el respeto de la privacidad viene siendo, en los últimos años, una prioridad de la Unión Europea y, evidentemente, de España (Vázquez Ruano, 2002). En este sentido, 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 se ha ocupado de los mismos.

El actual artículo 5.3 de la Directiva sobre intimidad y comunicaciones electrónicas aborda la cuestión de las tecnologías que permiten almacenar información u obtener acceso a la información ya almacenada en el terminal de un abonado o usuario. Tal precepto es tecnológicamente neutro, por lo que es aplicable no sólo a las *cookies* sino también a cualquier otra tecnología utilizada para acumular información o acceder a información almacenada en el equipo terminal de las personas. Un ejemplo de la aplicación del artículo 5.3 son el uso de tecnologías tales como los "programas espía" -programa ocultos de espionaje- y caballos de Troya -programas ocultos en mensajes o en otros programas, en apariencia, inocuos-. La finalidad de estas tecnologías varía enormemente. Mientras que, por un lado, unas son perfectamente inocuas e, incluso, útiles para el usuario, por otro lado, otras son claramente perniciosas y amenazadoras.

De acuerdo con el artículo 5.3 mencionado, por un lado, hay que facilitar a los usuarios de Internet información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE, y, por otro, debe reconocerse a los usuarios de Internet el derecho a negarse al tratamiento de los datos, es decir, que pueden oponerse a que se trate información obtenida de sus terminales.

A nivel nacional, se ha ocupado de la cuestión que examinamos la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico -LSSI-CE-, si bien la regulación que ésta última efectúa no es del todo feliz. En efecto, el legislador español ha transpuesto la norma comunitaria enunciada a través del párrafo segundo del art. 22 LSSI-CE. En éste se establece que el prestador de servicios de la sociedad de la información que utilice, en los terminales informáticos, técnicas que posibiliten el tratamiento y recuperación de datos debe cumplir con el deber de información a los sujetos afectados pudiendo éstos últimos oponerse a ello.

En cuanto a las críticas que cabe efectuar, entendemos poco correcta su ubicación sistemática, pues debemos considerar que se regulan dentro del título dedicado a las comunicaciones comerciales no solicitadas, cuando ni las *cookies* ni el *spyware* lo son. Desde el punto de vista sustantivo, destaca la parquedad de los términos en los que el legislador se pronuncia. Todo parece indicar que es lo mínimo que podía hacer, para cumplir con la obligación de transponer la normativa comunitaria, pues no tiene en cuenta las particularidades que, tanto las *cookies* como el *spyware*, presentan. Así, respecto a las *cookies*, debería haberse impuesto al prestador de servicios la obligación de informar sobre ellas, mediante un mensaje emergente o condicionar el acceso a la página que activa la *cookie* a la lectura de un aviso legal donde se informe sobre su existencia y demás condiciones de utilización de la página (Guerrero Picó, 2006).

En línea con la última apreciación formulada, debemos traer a colación la modificación operada, por parte de la Directiva 2009/136 sobre el art. 5.3 de la Directiva sobre privacidad y comunicaciones electrónicas, que obligará al legislador español a tomar en consideración su nuevo contenido que habrá de ser transpuesto, a más tardar, el 25 de mayo de 2011. El tenor actual del precepto -tras la citada reforma- determina que "los Estados miembros velarán porque únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos". El considerando 25 de la Directiva sobre privacidad requiere que las explicaciones se den de forma clara y precisa. Afirmaciones como, a título de ejemplo, que *los anunciantes y otras partes pueden también utilizar sus cookies o etiquetados* son absolutamente insuficientes. Técnicamente existen diversos y múltiples modos de proporcionar información y sería conveniente incentivar la creatividad en este campo.

Ha de observarse que el actual art. 5.3 de la Directiva sobre privacidad incide en una cuestión sobre la que la versión anterior no se pronunciaba -como tampoco lo hacía el art. 22 LSSI-CE-. Nos referimos a que expresamente se dispone que el consentimiento se deberá otorgar después –nótese la inclusión de tal término- de que el prestador de servicios haya informado al usuario, de forma sencilla y completa, sobre los fines del tratamiento de los datos. Actualmente, la configuración, por defecto, de tres de los cuatro navegadores más utilizados para Internet está predeterminada para aceptar todas las *cookies*. En esos casos, se envían *cookies* y se recoge información sin recabar consentimiento, lo que, a todas luces, contradice la necesidad de consentimiento previo. Debe entenderse, por consiguiente, que no cambiar la configuración establecida, por defecto, no puede ser considerado, en la mayoría de los casos, como consentimiento válido del usuario. Además, las redes de publicidad -que son entidades que realizan segmentación de audiencia mediante los perfiles de navegación de los usuarios para ofrecerles publicidad personalizada- y los editores de sitios *Web* que ofrezcan este tipo de publicidad deben proporcionar información sobre la finalidad del seguimiento, de manera clara y comprensible, para que los usuarios puedan tomar decisiones informadas sobre si quieren que su comportamiento de navegación sea monitorizado.

Con respecto a la información que debe darse sobre la publicidad comportamental -a la que, dicho sea de paso, el art. 5.3 *in fine* alude con la necesidad de informar al usuario sobre "los fines del tratamiento de los datos"-, los usuarios deben recibir información, entre otras cosas, de la identidad del proveedor de la red de publicidad y el objetivo del tratamiento de sus datos. Debe informarse

claramente al usuario de que las *cookies* permitirá al proveedor de publicidad, entre otras cosas, recoger información sobre sus visitas a otros sitios *Web*, los anuncios que éstos muestran, los anuncios en los que ha cliqueado, el tiempo empleado, etc.

A pesar de la modificación recientemente operada, no debe olvidarse que el considerando 66 de la Directiva sobre privacidad en las comunicaciones electrónicas señala que el consentimiento del usuario puede expresarse utilizando la configuración adecuada de un buscador u otras aplicaciones "cuando sea técnicamente posible y eficaz, con arreglo a las disposiciones correspondientes de la Directiva 95/46/CE". Tal extremo no supone una excepción al artículo 5.3, sino un recordatorio de que, en dicho entorno tecnológico, el consentimiento puede otorgarse de formas diferentes, cuando sea técnicamente posible y eficaz, de acuerdo con los demás requisitos pertinentes del consentimiento válido. En este contexto, una cuestión relevante es la de fijar las condiciones en que la configuración del buscador cumple los requisitos de la Directiva 95/46/CE, constituyendo, a tenor de la Directiva 95/46/CE, un consentimiento válido.

Habida cuenta de la relevancia que ostenta la configuración del buscador, a efectos de que los usuarios otorguen su consentimiento al almacenamiento de *cookies* y al tratamiento de la información que éstas suponen, es significativo que los buscadores dispongan de la configuración de no aceptación y no transmisión de *cookies* de terceros. Para complementar este último aspecto y, con carácter simultáneo, hacerlo más eficaz, los buscadores deberían pedir a los usuarios que entrasen en un asistente de privacidad la primera ocasión que instalen o actualicen el buscador y proporcionarles un método fácil de ejercer su opción durante la utilización del producto.

Es preceptivo, por consiguiente, que exista un consentimiento informado, por parte del usuario, para la utilización de *cookies* publicitarias. Para su incorporación al ordenamiento español existen entidades, como *Interactive Advertising Bureau* -IAB-, que han propuesto la adopción de una solución internacional que implique el uso de un icono común para todo el sector de la publicidad digital -siguiendo, en cierto sentido, la iniciativa adoptada por la industria estadounidense en enero de 2010-. Tal icono podría, asimismo, alertar a los consumidores, no sólo del hecho de que un proveedor de redes de publicidad está controlando sus búsquedas por Internet para enviar publicidad según sus presumibles preferencias, sino también para, si el usuario lo desea, optar por revocar el consentimiento inicialmente prestado.

Debe considerarse que los problemas relativos a la obtención de consentimiento fundamentado aumentan aun más, si cabe, en el caso de los menores de edad. Además de los requisitos descritos, para que exista consentimiento respecto a los niños, deben prestarlo sus padres o, en su caso, sus representantes legales. En el supuesto que nos ocupa, esto supone que los proveedores de redes de publicidad podrían tener que informar a los padres de la recogida y utilización de datos del niño y obtener su consentimiento antes de recoger dichos datos y seguir utilizando la información con fines de realizar publicidad a medida para niños.

En definitiva, entendemos que, a fecha de hoy, el proceder de la mayor parte de los proveedores de redes de publicidad, en la cuestión que comentamos, no ha sido, precisamente, el establecido en el actual art. 5.3 de la Directiva sobre privacidad. Con las nuevas exigencias legales impuestas, a nuestro juicio, el usuario estará más informado y será, si cabe, más consciente de que se está analizando su comportamiento.

Las técnicas aludidas de monitorización del comportamiento se emplean, como ya hemos adelantado, con fines publicitarios. En otras palabras, la publicidad virtual basada en el comportamiento se fundamenta en el seguimiento continuo de ciertos usuarios en base a su navegación por determinados sitios *Web*. Tal control, como hemos visto, se opera, entre otras prácticas, por medio de las *cookies* de rastreo -*tracking cookies*- que recopilan información sobre el comportamiento de navegación de los individuos para ofrecerles anuncios personalizados. Estas actuaciones pueden

suponer violaciones de la privacidad. Por ello, el Grupo de Trabajo del artículo 29, en el dictamen 2/2010, de 22 de junio de 2010, entiende que, aunque se trata de herramientas que pueden aportar notables ventajas a la industria -y eventualmente a los usuarios-, comprometen la privacidad.

4. LA AUTORREGULACIÓN COMO COMPLEMENTO DE LA NORMATIVA LEGAL

Además de las medidas de carácter normativo mencionadas, no debe obviarse las iniciativas fruto de la autorregulación de la industria, pues constituyen un sugerente complemento de aquéllas. Representan, en este sentido, un paradigma de referencia en la materia, al menos, las dos siguientes: 1) *Interactive Advertising Bureau Europe* -IAB Europe- elaboró, en mayo de 2009, *Social Advertising Best Practices* fundamentado en ciertos principios; 2) El Documento de buenas prácticas denominado *Global Principles for Online Behavioral Advertising*, elaborado en julio de 2009, por determinadas instituciones norteamericanas -en particular la *American Association of Advertising Agencies*, la *Association of National Advertisers*, el *Council of Better Business Bureau*, la *Direct Marketing Association* y el *Interactive Advertising Bureau*- relativas a la publicidad comportamental. Resulta conveniente que las prácticas mencionadas en estos documentos inspirasen los sistemas nacionales de autorregulación.

El texto relativo a las mejores prácticas en el ámbito de la publicidad -*Social Advertising Best Practices*- elaborado por IAB Europe se fundamenta en cinco principios: 1) Antes de proceder al envío de publicidad social el consumidor debe prestar necesariamente su consentimiento; 2) Los consumidores han de estar suficientemente informados del uso que se dé a sus datos y, en su caso, deben poder solicitar su baja; 3) Habrá de informarse al consumidor sobre el hecho de que un tercero pueda tener acceso a su información; 4) Deberán implementarse medidas de seguridad en el supuesto de que en el perfil creado para la publicidad social se incluyan datos personales y; 5) Con carácter previo a distribuir el anuncio en la red social los anunciantes deberán poner a disposición de los consumidores una vista previa sobre cómo será utilizada su información dentro del anuncio.

El segundo documento mencionado de carácter voluntario -*Global Principles for Online Behavioral Advertising*- desarrolla los siete principios que, en febrero de 2009, propuso la *Federal Trade Commission*, que son aplicables a la publicidad comportamental de carácter virtual. Esta última puede definirse, según el texto que citamos, como aquella que se basa en la recopilación virtual de información, relativa a los hábitos de navegación en Internet, con el objetivo de emplear dicha información para predecir las preferencias o intereses del usuario y proceder al envío de publicidad a un determinado ordenador o dispositivo basada en las preferencias o intereses que se deducen del comportamiento del usuario. Para la efectiva protección del consumidor resultan básicos los principios de transparencia y de control o verificación, por parte del consumidor, en base a los cuales se debe permitir a aquél decidir sobre la captación y uso de información a efectos de la publicidad comportamental. Además de los mencionados principios, el documento que analizamos alude a cinco más de carácter vital, a saber: educación del consumidor; seguridad y retención limitada de los datos; estabilidad de las políticas de privacidad -siendo, para los cambios, preceptivo el previo consentimiento del usuario-; datos sensibles -será preciso un consentimiento diferenciado tanto para datos especialmente sensibles como para los menores de edad-; y responsabilidad tanto en la aplicación del documento como en la resolución de eventuales reclamaciones.

5. REFERENCIAS BIBLIOGRÁFICAS

BASKIN, B.; PILTZECKER, T. (2006): *Combating spyware in the enterprise*, Syngress.

BENNETT, C.J. (2001): "Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web", *Ethics and Information Technology*, Vol. 3, nº 3, pp. 197-210.

BENSOUSSAN, A. (1998): *Internet, aspects juridiques*, 2ª edición, Hermes, París.

BIGNÉ ALCANIZ, J. E.; RUIZ MAFÉ, C.; ANDREU SIMÓ, L. (2005): "Satisfacción y lealtad del consumidor on line". En GUTIÉRREZ ARRANZ, A.M.; SÁNCHEZ-FRANCO, M.J. (Coords.), *Marketing en Internet. Estrategia y empresa*, Pirámide, Madrid, pp. 201-235.

BRUENING, P. J.; STEFFEN, M. (2004): "Spyware: Technologies, Issues, and Policy Proposals", *Journal of Internet Law*, Vol. 7, nº 9, pp. 3-8.

CROLL, A.; POWER, S. (2009): *Complete web monitoring*, O'Reilly Media.

D´ORAZIO, R. (1999): "Dati personali in rete aperta". En CUFFARO, V.; RICCIUTO, V. (Eds.), *Il tratamento dei dati personali*, Vol. 2, Giappichelli, Torino, pp. 278-280.

ERDOZÁIN LÓPEZ, J.C. (2007): "La protección de los datos de carácter personal en las telecomunicaciones", *Aranzadi Civil*, nº 2, pp. 1845-1889.

FERNÁNDEZ RODRÍGUEZ, J.J. (2004): *Secreto e intervención de las comunicaciones en Internet*, Thomson Civitas, Madrid.

FERNÁNDEZ TERUELO, J.G. (2007): *Cibercrimen. Los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, Asturias.

GOLUMBIC, M.C. (2008): *Fighting terror online: The convergence of security, technology, and the law*, Springer.

GRIMALT SERVERA, P. (2004): "La contratación en masa en Internet: El consentimiento de los consumidores para el tratamiento de sus datos en una condición general". En MORO ALMARAZ, M.J. (Dir.) y APARICIO VAQUERO, J.P.; BATUECAS CALETRÍO, A. (Coords.), *Autores, consumidores y comercio electrónico*, Colex y Caja Duero, Madrid, pp. 235-249.

GUERRERO PICÓ, M.C. (2006): *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson Civitas, Madrid.

GUILLÉN CATALÁN, R. (2005): *Comunicaciones comerciales no solicitadas*, Thomson Aranzadi, Navarra.

GUTIÉRREZ GONZÁLEZ, P.P.; PEDREIRA SÁNCHEZ, D.; VELO MIRANDA, M. (2005): *Diccionario de la publicidad*, Editorial Complutense, Madrid.

HARDING, W.T.; REED, A.J.; GRAY, R.L. (2001): "Cookies and Web Bugs: What they are and how they work together", *Information Systems Management*, Vol. 18, nº 3, pp. 17-24.

JANCZEWSKI, L.J.; COLARIK, A. (2008): *Cyber warfare and cyber terrorism*, Idea Group.

JAWAHITHA, S. (2004): "Consumer protection in E-commerce: Analyzing the Statutes in Malasya", *Journal of American Academy of Business*, Vol. 4, nº 1-2.

JUILIÁ BARCELÓ, R. (2000): "Cookies, perfiles, direcciones IP: Cuestiones pendientes en la legislación sobre protección de datos", *Novática*, nº 148, pp. 20-23.

KLANG, M. (2003): "Spyware: Paying for software with our privacy", *International Review of Law Computers & Technology*, Vol. 17, nº 3, pp. 313-322.

KUSSMAUL, W. (2007): *Own Your Privacy: Privacy and security are not antithetical*, PKI Press.

LEVINE, J.R.; LEVINE, M. (2010): *The Internet for dummies*, 12ª ed., Wiley Publishing, Indiana.

LLÁCER MATACÁS, M.R. (2003): "La protección de los datos personales en Internet". En BARRAL VIÑALS, I. (Coord.), *La regulación del comercio electrónico*, Dykinson, Madrid, pp. 157-190.

MADRID PARRA, A. (2008): "Protección de datos personales en el comercio electrónico". En *Derecho de la Empresa y Protección de Datos*, Thomson Aranzadi y Agencia Española de Protección de Datos, Navarra.

MARTÍN, D.; WU, H.; ALSAID, A. (2003): "Hidden surveillance by Web sites: Web bugs in contemporary use", *Communication of the ACM*, Vol. 46, nº 12, pp. 258-264.

MARTÍNEZ MARTÍNEZ, M.; FERNÁNDEZ RODRÍGUEZ, F.; SACO VÁZQUEZ, M. (2008): *Supermercados.com. Marketing para los supermercados virtuales*, Esic, Madrid.

MUÑIZ CASANOVA, N.; ARIZ LÓPEZ DE CASTRO, E. (2004): "Los datos personales en el desarrollo de la actividad". En MARZO PORTERA, A.; RAMOS SUÁREZ, F.M. (Dirs.): La *Protección de Datos en la Gestión de Empresas*, Thomson Aranzadi, Navarra, pp. 85-118.

NABBALI, T.; PERRY, M. (2003): "Going for the throat: Carnivore in an Echelon World - Part I", *Computer Law and Security Report*, Vol. 16, nº 9, pp. 456-467.

NGAI, E.W.; WAT, F.K. (2001): "A literature review and classification of electronic commerce research", *Information and Management*, nº 39, pp. 415-419.

PALMER, D.E. (2005): "Pop-Ups, cookies, and spam: Toward a deeper analysis of the ethical significance of Internet marketing practices", *Journal of Business Ethics*, Vol. 58, nº 1, pp. 271-280.

PAYERAS CAPELLÁ, M.M. (2005): "Los tratamientos invisibles de información (las *cookies*): perspectiva técnica y análisis jurídico". En *Marketing y publicidad en Internet*, Universitat de les Illes Balears y Universitat Oberta de Catalunya, Barcelona, pp. 41-63.

PAYERAS CAPELLA, M.M.; FERRER GOMILLA, J.L. (2004): "Explicación técnica de las amenazas de las TIC a la intimidad". En GÓMEZ MARTÍNEZ, C. (Dir.): *Derecho a la intimidad y nuevas tecnologías*, Consejo General del Poder Judicial, Madrid, pp. 77-106.

PIQUERES CASTELLOTE, F. (2006): "Conocimientos básicos en Internet y utilización para actividades ilícitas". En VELASCO NÚÑEZ, E. (Dir.): *Delitos contra y a través de las nuevas tecnologías ¿cómo reducir su impunidad?*, Consejo General del Poder Judicial, Madrid, pp. 41-88.

RADCLIFF, D. (2004): "Spyware", *Network World*, Vol. 21, nº 4.

RIBAS ALEJANDRO, X. (1999): "Marketing y publicidad en Internet", *Revista Autocontrol de la Publicidad*, nº 28.

RICO CARRILLO, M. (2003): *Comercio electrónico, Internet y Derecho*, Legis, Caracas.

SCHULTZ, E. (2003): "Pandora's Box: Spyware, Adware, Autoexecution, and NGSCB", *Computers & Security*, Vol. 22, nº 5.

SCHWARTZ, P.M. (2004): "Property privacy and personal data", *Harvard Law Review*, Vol. 117, pp. 2055-2128.

SERRA RODRÍGUEZ, A. (2000): "Los derechos de los particulares en la nueva Ley de protección de datos de carácter personal", *La Ley*, Vol. 6.

SHARMA, A.; SHET, J. (2004): "Web based marketing the comino revolution in marketing thought and strategy", *Journal of Business Research*, nº 57, pp. 696-702.

SIPIOR, J.C.; WARD, B.T.; ROSELLI, G.R. (2005): "The ethical and legal concerns of spyware", *Information Systems Management*, Vol. 22, nº 2, pp. 39-49.

STAFFORD, T.F.; URBACZEWSKI, A. (2004): "Spyware: the ghost in the machine", *Communications of the Association for Information Systems*, Vol. 14, pp. 291-306.

TREESE, G.W.; STEWART, L.C. (2003): *Designing systems for Internet commerce*, Addison-Wesley.

URBACH, R.R.; KIBEL, G.A. (2004): "Adware/Spyware: An update regarding pending litigation and legislation", *Intellectual Property & Technology Law Journal*, Vol. 16, nº 7, pp. 12-16.

VALERO TORRIJOS, J. (2003): "El uso de *cookies* por las Administraciones Públicas. Una interpretación desde la normativa española sobre protección de datos personales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 3, pp. 173-178.

VÁZQUEZ RUANO, T. (2002): "Aproximación jurídica al *Spam* desde la protección de datos de carácter personal", *Revista de la Contratación Electrónica*, nº 33.

VOLKMER, C.J. (2004): "Should adware and spyware prompt congressional action?", *Journal of Internet Law*, Vol. 7, nº 11, pp. 1-8.

WENZ, C. (2001): *Active Server Pages*, Marcombo.