Ciencias Económicas 29-No. 2: 2011 / 175-190 / ISSN: 0252-9521

LAS COOKIES COMO INSTRUMENTO PARA LA MONITORIZACIÓN DEL USUARIO EN LA RED: LA PUBLICIDAD PERSONALIZADA

David López Jiménez[1]

ÍNDICE

RESUMEN

En Internet acontecen prácticas publicitarias que,pasando desapercibidas para el usuario, pueden vulnerar su privacidad. Una de ellas es el recurso, por parte de numerosas empresas que operan en la Red, a técnicas susceptibles de monitorizar la actuación del usuario como las *cookies*. Éstas últimas pueden tener diversas utilidades, entre las que destaca la posibilidad de remitir anuncios comerciales electrónicos personalizados a los gustos y preferencias de quienes los visualizan.

PALABRAS CLAVE: ADMINISTRACIÓN DE LA RELACIÓN CON EL CLIENTE;COOKIES; INTERNET; NAVEGADOR; NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

1. Doctor (con mención europea) en Ciencias Económicas y Empresariales y Doctor en Derecho. Grupo de Investigación de Excelencia GITICE (Universidad de Huelva). dlopez3@us.es; dlopezjimenez@gmail.com.

SUMMARY

Sometimes, advertising practices occur on the Internet not allowing a user to notice that the privacy is not being respected. One way, used by some of the companies that work on the Web, is to control the actions made by the user throw different resources, like for example the cookies. The latter can have different utilities, being one of the most important uses, the possibility to send commercial electronic announcements according to the preferences of those who visualize them.

KEY WORDS: CUSTOMER RELATIONSHIP MANAGEMENT;COOKIES; INTERNET; NAVIGATOR; NEW INFORMATION AND COMMUNICATIONS TECHNOLOGIES.

1. INTRODUCCIÓN

La irrupción de Internet ha supuesto, en un breve lapso temporal, un elenco muy significativo de cambios en el plano comercial. Uno de ellos es, qué duda cabe, el ámbito publicitario. En efecto, tal canal posibilita el acceso, con independencia de su naturaleza y/o tamaño, a todo tipo de empresas. Así, a título de ejemplo, podrían acceder, en igual de condiciones y con niveles de efectividad similares, tanto pequeñas y medianas empresas como grandes empresas nacionales e, incluso, multinacionales.

La comunicación comercial se erige en un elemento esencial para la lucha competitiva por la conquista del mercado (Ascarelli, 1970; Font Galán, 1987). En sus orígenes, la publicidad difundida en Internet era muy básica. De hecho, al principio, se operó una suerte de informatización de la publicidad sin tener en consideración las especiales particularidades de Internet (Romero Calmache y Banjul Peyró, 2010). Sin embargo, con el transcurrir de los años, se diseñaron formatos publicitarios adaptados tanto al canal como al usuario del mismo (Ferrer, 2001). Asimismo, como veremos, se idearon diversas técnicasque permiten una alta segmentación de la audiencia, así como mensajes más afines a las necesidades del usuario al que la publicidad se remite.

Cada vez en mayor medida, son más las empresas que, para remitir ofertas comerciales personalizadas,recurren a ciertas técnicas de monitorización del comportamiento de los usuarios de Internet. En este sentido, destaca el caso de las *cookies* que, como veremos, facilitan el tratamiento invisible de un elenco relevante de datos personales. Para tomar conciencia de la enorme relevancia que, en la práctica, presentan, veremos su concepto, clasificación, así como distinción de otras figuras que persiguen hacerse con información personal de los usuarios. No perderemos de vista la regulación normativa aprobada en el espacio comunitario y español para poner freno a este tipo de herramientas.

Antes de analizar, con cierto grado de detalle, tal práctica electrónica, dirigida a monitorizar el comportamiento de los internautas, haremos algunas alusiones de carácter general sobre el fenómeno publicitario tradicional y virtual. Asimismo, nos detendremos en diferentes técnicas virtuales dirigidas a la creación de perfiles de los potenciales consumidores y/o usuarios de la Red.

2. CONSIDERACIONES GENERALES EN TORNO A LA PUBLICIDAD TRADICIONAL Y VIRTUAL

La publicidad representa un fenómeno característico de la sociedad actual que ha incrementado, de manera considerable, su actual trascendencia social y económica y presumiblemente así acontecerá en el futuro. Constituye una actividad que desempeña un papel muy relevante. Así, entre otros aspectos, estimula el crecimiento y la innovación, impulsa la competitividad, combate los abusos de posición dominante, y amplía las posibilidades de elección del consumidor. Para cumplir esta importante misión, la publicidad debe disfrutar de un alto nivel de confianza por parte de este

último. A tal fin, es necesario que la misma sea veraz, legal, honesta y leal.

Asimismo, es un instrumento competitivo, de los más significativos de la sociedad contemporánea (Alpa, 1986; Suárez Villegas y Pérez Chica, 2002), que los operadores económicos utilizan en el tráfico para promover la contratación sobre los bienes y/o servicios que ofertan en el mercado (Armstrong, 2002; Carvajal y Barthe, 2002; Farré López, 2003). Es un claro ejemplo de información asimétrica (Morales Moreno, 1988). De hecho, la exigencia de que la información sea veraz permite reprimir las expresiones publicitarias que incluyen alegaciones falsas, suponiendo, de este modo, un abuso de la asimetría en la información entre anunciante y receptor del mensaje comercial. También ha de repararse en que la publicidad no sólo expone los caracteres de los productos y/o servicios, sino que va más allá. En efecto, se configura como un medio que transmite, inculca y exalta determinados valores y pautas de conducta estimados como la base común de la conciencia colectiva.

Tal actividad no solo es información (Pino Abad, 1991; Corredoira y Alfonso, 1994) –ni siquiera hoy tiene el máximo protagonismo-, sino que prima la persuasión (Ghidini, 1968; Font Galán, 1990; Muñoz Machado, 1994; Qualter, 1994; Domínguez Pérez, 1999; Haan 2000; Stazi, 2004). A través de esta última, el fenómeno publicitario presenta connotaciones de agresividad, dado que, en la actualidad, la competencia económica de los empresarios se realiza a través de la publicidad (Beater, 2000; Spang, 2005). La finalidad persuasiva, propia del denominado modo publicitario como modalidad formal típica de los mensajes publicitarios, menoscaba la objetividad que es característica de la información, aunque el predominio de una u otra dimensión dependen de la expresión publicitaria concreta. En esta línea, cierto sector apunta que, frente a los mensajes puramente informativos, la comunicación publicitaria actual va unida a una intensa actividad creativa (Bassat, 2003).

Ahora bien, frente al modelo de publicidad centrado en informar y persuadir a los destinatarios sobre la primacía de los bienes y/o servicios del anunciante frente a los de otros, en la actualidad adquiere enorme importancia las estrategias publicitarias en la Red que, precisamente, buscan que los potenciales consumidores y/o usuarios –o, en términos generales, los comúnmente denominados internautas- tengan la impresión de que la empresa anunciante tiene un proyecto de futuro y, a su vez, es dinámica. Para alcanzar tal extremo en Internet se recurre, en gran medida, a anuncios caracterizados por su originalidad (Hall, 1997).

La mala publicidad –que no cumpla todos o alguno de los mencionados caracteres- aunque represente una porción minúscula respecto al conjunto total, irá socavando la confianza del consumidor y toda publicidad acabará, de una u otra manera, sufriendo las desfavorables consecuencias. Por ello, en beneficio de toda la sociedad, para que no acontezca este último extremo, es preciso que la publicidad en general esté regulada. Existen dos opciones, que no son excluyentes sino complementarias, a saber: la regulación normativa –o heterorregulación- y la autorregulación –o disciplina de la propia industria-.Aunque ambas disciplinan, en mayor o menor medida, aluden a las técnicas publicitarias susceptibles de vulnerar la privacidad del usuario, la autorregulación elaborada por la industria, por sus ventajas inherentes, suele ir por delante de la norma legal. Si bien es cierto que la publicidad personalizada puede implicar un gran número de ventajas para los empresarios que hacen uso de las mismas, también debe reconocerse que, en numerosas ocasiones, puede, simultáneamente, suponer una violación de los derechos del usuario. Para, precisamente, garantizar el respeto de la protección de datos de carácter personal en la materia tanto el legislador como la propia industria –en virtud de la autorregulación-, insistimos, han aprobado un elenco de normas al respecto.

3. DE LA PUBLICIDAD DECIMONÓNICA A LOS NUEVOS PARÁMETROS INHERENTES A LAS NOVEDOSAS TECNOLOGÍAS PUBLICITARIAS: LA CREACIÓN DE PERFILES DE POTENCIALES CLIENTES

Una de las manifestaciones más significativas que las Tecnologías de la Información

y de la Comunicación han supuesto, a nivel empresarial, se observa en la publicidad interactiva. Para que esta última sea más eficaz y eficiente se han puesto en práctica novedosas técnicas (caracterizadas básicamente por su bajo coste, rapidez y capacidad de llegar a un alto número de usuarios) que tienen como finalidad captar la atención integral de los receptores. Puede, a tal efecto, afirmarse, siguiendo a cierto sector de la literatura académica (Azlor Villa, 2001; García Uceda, 2001; López Lita, 2004; Checa Godoy, 2007), que el sistema de promoción tradicional ha perdido valor en beneficio del virtual.

Toda empresa que, en la actualidad, pretenda perdurar en el mercado competitivo global debe incorporar las nuevas tecnologías en su actividad cotidiana, para estar permanentemente adecuada a las tendencias de venta, a través de los nuevos medios tecnológicos, y poder diseñar estrategias de marketing electrónico. La necesidad de las empresas de mantener los clientes y de estrechar relaciones con los mismos –marketing relacional- determina que aquellas busquen formas de llegar directamente al consumidor individual, personalizando la oferta, constituyendo, de esta manera, novedosos tipos de venta que permiten que las empresas establezcan relaciones continuadas y directas con el mismo, esté donde esté (San Martín Gutiérrez y López Catalán, 2010).

A finales del siglo XX, algunos autores (Peppers y Rogers, 1999) determinaron que la publicidad en Internet, cuyo origen se sitúa a principios de los años noventa (Kaye y Medoff, 2001), constituía una transformación radical del paradigma de marketing, que evolucionó desde un modelo predominantemente unidimensional a otro totalmente interactivo con relaciones uno a uno personalizadas, que progresivamente está alcanzando más protagonismo (Perlado Lamo de Espinosa, 2006; López de Aguileta y Torres Romay, 2007).

Cabe referirse al recurso, cada vez más acusado, a técnicas, que tienen como fin configurar el perfil personal de los usuarios, para, precisamente, lograr la fidelización de los mismos con respecto a determinadas tiendas virtuales. Nos referimos, entre otras, al *database marketing*, *data mining*, *computerprofiling* y el *frontendverification*.

Respecto al *database marketing* (o marketing de base de datos), cabe decir que está especialmente vinculado con la relación que se suscita entre el anunciante y el receptor de la publicidad (Fletcher,Wheelery Wright, 1991). Busca desarrollar una base de datos que incluya tanto a los consumidores actuales como a los potenciales. Constituye, en todo caso, una técnica a la que hace varios años se opuso la Comisión Nacional de Informática y Libertades radicada en Francia, por su previsible vulneración de la privacidad (Ramonet, 2002). La finalidad de esta relevante autoridad administrativa independiente es vigilar que la informática esté al servicio del ciudadano y no vulnere la identidad humana, ni los derechos humanos, la intimidad o las libertades individuales o públicas.

El *data mining* (o minería de datos), que prepara, sondea y explora los datos, para sacar la información oculta presente en los mismos, persigue hacerse con determinada información personal de los potenciales consumidores y/o usuarios para promocionar ciertos productos y/o servicios (Hand, 1998; Mena, 1999). Así, por ejemplo, mediante esta técnica se analiza el comportamiento de los visitantes en un sitio *Web*, y, sobre la base de los productos adquiridos por los consumidores con anterioridad, se les oferta otros en los que, en atención a su perfil, se prevé que pudieran estar interesados.

El *computerprofiling* permite efectuar una combinación de datos elementales que aisladamente considerados no significarían nada, por lo que pasarían desapercibidos para los anunciantes, pero que relacionados dan la oportunidad de conocer perfiles comerciales de los clientes (Ford, 2000).

Finalmente, la práctica denominada *frontendverification* es utilizada para contrastar la exactitud de la información personal cotejándola con informaciones similares almacenadas en bases de datos informáticas generalmente de terceros(Clarke, 1994).

La utilización de estas técnicas puede limitar drásticamente el grado de control de los afectados sobre las informaciones que les conciernen, ya que, en muchos casos, la interacción de estas

herramientas elabora aproximaciones basadas en datos personales cruzados con estadísticas que su propio titular ignora.

Como podrá suponerse, la publicidad interactiva, que, en ciertos supuestos, habrá recurrido a prácticas como las que acabamos de enunciar, podrá presentar, sin contar con el previo consentimiento del afectado, carácter personalizado, siendo ilícita, pues vulnerará los derechos de los consumidores y/o usuarios(Herrero-Tejedor Algar, 1998; Nivarra y Ricciuto, 2002; Vicenti, 2003).

Además de las técnicas examinadas, para la adecuada personalización y segmentación del correo electrónico con fines comerciales se hará uso tanto de un determinado *software* como de una completa base de datos con los que se personalizará el contenido dentro del cuerpo del mensaje (Campuzano Tomé, 2000; Lavilla Raso, 2002). Las herramientas de CRM -*CustomerRelationship Management* o Administración de la Relación con el Cliente- proveen de información sobre los gustos o comportamientos de compra de los posibles destinatarios, por lo que se consigue adaptar, de manera automática, el mensaje al perfil específico del *target group* o público objetivo al que se dirige. Tal extremo facilitará, naturalmente, la segmentación, la personalización (Méndiz Noguero, 2000), incrementará notablemente la calidad del servicio y mejorará los resultados de la campaña (Ansari y Mela, 2003; Chittenden y Rettie, 2003; Guillén Catalán, 2009).

La materia que abordamos determina que analicemos, de forma somera, las diversas fuentes o mecanismos, en virtud de los que pueden recabarse los datos de carácter personal, que, posteriormente, se emplearán para la remisión de comunicaciones comerciales electrónicas. Así, podemos discernir dos grandes grupos. En el primero, los datos que la empresa posee del titular de los mismos, se debe bien a un acto voluntario, por el que se cumplimentó un determinado formulario, bien a la previa existencia de una relación contractual. En el segundo, los datos personales del titular no se conocen por el hecho de que éste haya prestado, consciente y voluntariamente, su consentimiento a tal efecto, sino que obedecen al recurso de otros medios cual, por ejemplo, el uso de técnicas electrónicas, que veremos en el siguiente apartado.

Ahora bien, también ha de tomarse conciencia que en el proceso de personalización del mensaje ocupará una posición muy significativa las denominadas cookies de las que nos ocuparemos seguidamente.

4. LAS COOKIES COMO HERRAMIENTAS PARA LA REMISIÓN DE PUBLICIDAD ON-LINE PERSONALIZADA

Entre los instrumentos técnicos a los que más se recurre, en la actualidad, en Internet, para la personalización del mensaje comercial destacan las denominadas *cookies*. Aunque su uso puede resultar plenamente legítimo, si se respetan los presupuestos legales establecidos, pueden llegar a suponer una vulneración de la privacidad. Seguidamente, nos ocuparemos de su concepto, modalidades, distinción de figuras parcialmente afines, así como la situación legislativa imperante tanto en el plano comunitario como español.

4.1. Concepto

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; Sharma y Shet, 2004; BignéAlcaniz, Ruiz Mafé y Andreu Simó, 2005), pues, en muchas ocasiones, no habrá resultado, en absoluto, conocida ni, mucho menos, consentida (Juliá Barceló, 2000; LlácerMatacás, 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) cuales, entre otros, son, las *cookies*, troyanos, *spyware* y *web bugs*. Además de los métodos de rastreo mencionados, procede referirse a

la configuración del equipo –resolución de pantalla, idioma, colores, sistema operativo, navegador, versión del mismo, y un largo etcétera- que se conecte a Internet que, sin recurrir a las prácticas anteriores, por sí mismo, revela cuantiosos datos personales. Este último extremo fue puesto de manifiesto a través del estudio denominado *Panopticlick* que pone de relieve que los navegadores, sin que los usuarios lo sepan, dejan una huella única que los hacen inconfundibles en Internet. Algo que, si se nos permite la expresión, podría ser calificado como el "ADN digital". Las herramientas disponibles van más allá, dado que existen ciertos programas que efectúan búsquedas en Internet con la finalidad de acumular datos personales. En este último sentido, una noticia publicada en el *Minneapolis StarTribune* ponía de manifiesto cómo se podía elaborar una detallada bibliografía de una persona elegida al azar, utilizando tanto esos programas a los que aludíamos como la información recogida en los grupos de discusión de la Red en los que ese individuo participó. Ese periódico, en concreto, logró obtener la dirección de la persona, su número de teléfono, lugar de nacimiento, estudios, profesión, lugar de trabajo, aficiones, clase favorita de cerveza, restaurantes frecuentados y lugares de vacaciones.

De esta manera, podríamos considerar que, aunque un determinado usuario acometiera diversas actuaciones (como, por ejemplo, mecanismos que inhabilitaran el uso de *cookies* y/o recurrieran a una *proxy*-programa o dispositivo que realiza una acción en representación de otro., que ocultara la IP) para evitar ser identificado en la Red, su huella digital es prácticamente única, por lo que, superando tales barreras, podría ser rastreado. Por este motivo, los desarrolladores de navegadores de Internet deberían considerar qué pueden hacer para disminuir la posibilidad de elaborar huellas digitales, particularmente a nivel API –que se refiere a la interfaz de programación de aplicaciones- de *JavaScript*.

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 (Madrid Parra, 2008; MitjansPerelló, 2009).

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 nuestros efectos. Así, por lo que a seguridad se refiere, a finales de 2001, en el seno del proyecto *CyberKnight*, el FBI creó un virus, denominado *MagicLantern*, 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 *keylogging* que registrará las pulsaciones del teclado (Nabbali y Perry 2003; Kussmaul, 2007; Golumbic, 2008).

El potencial de esta información es enorme, desde la perspectiva del marketing (PayerasCapellá, 2005), 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; 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*pueden definirse como pequeños ficheros de texto, que algunos servidores *Web* piden al 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). 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.

4.2. Clasificación

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* 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. Las *cookies flash* o *Local SharedObject* –Objeto Local Compartido- constituyen una colección de archivos tipo *cookie* almacenadas como archivo en el ordenador del usuario. Se emplean por todas las versiones de *Adobe Fash Player*, desde la versión 6.0 y posteriores de Macromedia, hasta el *Flash MX Player*. Con la configuración por defecto, *Adobe Flash Player* no solicita el permiso del usuario para alojar las *cookies flash* en el disco duro.

Si bien la finalidad de esta tipología de *cookies* parece ser la misma que las que ostentan carácter tradicional –publicidad comportamental-, son, si cabe, más invasivas de la privacidad, dado que, entre otras actuaciones, pueden recuperar *cookies* tradicionales borradas previamente por el usuario. Un problema similar suscitan las denominadas *Evercookies* que, como se deduce de su propia denominación, son prácticamente imborrables. Se trata de una *cookie* persistente y prácticamente imborrable que, entre otros fines, podría emplearse para espiar a los usuarios de Internet. Representa una creación de *SamyKamkar* ideada en lenguaje *JavaScript* que produce huellas que vuelven a aparecer aunque el internauta quiera borrarlas. Para ello, utiliza ocho métodos de almacenamiento, camuflándose en los archivos ocultos o temporales del ordenador.

4.3. Distinción de figuras afines

Como hemos adelantado, cuando navegamos en la Red revelamos un elenco nada desdeñable de información sobre modelos de tráfico y, simultáneamente, sobre preferencias de contenido. Como también hemos manifestado,los datos de carácter personal ostentan un valor muy significativo, dado que,

entre otros factores, permitirán la remisión de comunicaciones comerciales electrónicas personalizadas. Asimismo, ha de advertirse que para el conocimiento de nuestros datos personales, lo que incluye gustos y preferencias, se recurre a ciertas aplicaciones electrónicas que, desapercibidas para el usuario, recopilarán nuestros datos de índole personal. Naturalmente, entre las mismas se encuentran las *cookies*, pero también existen otras muchas que necesariamente deben distinguirse. En este sentido, ha de hacerse alusión a los troyanos, *spyware* y *web bugs*.

En cuanto a los troyanos –como los *trapdoors*, *logicbombs* y *data diddling*-, 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. Las puertas falsas -*trapdoors*- 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. Las bombas lógicas –*logicbombs*-son similares a los troyanos, pero, mientras que un troyano comienza a funcionar cuando se ejecuta el programa que lo contiene, una bomba lógica únicamente se activa bajo ciertas condiciones, cual, entre otras, es 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. De hecho, puede permanecer inactiva en el sistema durante mucho tiempo, sin que, por consiguiente, existan indicios para sospechar un funcionamiento anómalo. Por último, cabe poner de manifiesto que tienen efectos destructivos sobre el *software* y *hardware*. Y, finalmente, La modificación de datos -*data diddling* o *tampering*- se refiere a la alteración desautorizada de datos o del *software* del sistema, incluyendo borrado de archivos.

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; Bruening y Steffen, 2004; Radcliff, 2004; Stafford y Urbaczewski, 2004; Volkmer, 2004). Podemos diferenciar tres grandes tipos de *spyware*: 1) el *snoopware*, que son los *keystrokeloggers* –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-normalmente proceden de aplicaciones electrónicas que se ofrecen gratuitamente a través de la Red-; 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.

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.

Los *mail bugs* son los *bugs* que se incluyen en los mensajes de correo electrónico. Cuando se procede a la visualización de estos últimos, la imagen se descargará del servidor. Al ser incorporadas a los correos electrónicos, 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.

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. 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 comunicacioneselectrónicas se ha ocupado de los mismos.

4.4. Regulación europea y española

El actual artículo 5.3 de la mencionada Directiva sobre intimidad y comunicaciones electrónicas aborda la cuestión de las tecnologías que permiten almacenar información u obtener acceso a la información almacenada en el terminal de un abonado o usuario. 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, 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. En este sentido, ciertos autores (Plaza Penadés, 2007) determinan que tal aspecto resulta especialmente significativo cuando otros usuarios, diversos al usuario original, tienen acceso al equipo y, a través de este, a cualquier dato sensible de carácter privado almacenado en el mismo.

A nivel español, 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 (en adelante 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 de la 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. Tendrían que haber sido disciplinadas en otro capítulo de la LSSI-CE o en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, o en la Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal -LOPD-. 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. No obstante, a fecha de hoy, únicamente dos países, como Dinamarca y Estonia, han notificado a la Unión Europea que implementarán las medidas necesarias para cumplir con la reforma de las telecomunicaciones. A *sensu contrario*, solo tales países se han comprometido a respetar las obligaciones establecidas por lo que a las *cookies* se refiere. Aunque otros Estados, como Francia, Eslovenia, Luxemburgo, y Reino Unido, han adoptado diversas medidas, a juicio de la Comisión Europea, son insuficientes.

El tenor actual del precepto 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 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 de la 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*. Debe entenderse 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. En todo caso, como veremos, esta tendencia está cambiando, dado que los navegadores están anunciando modificaciones relevantes al respecto.

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-.

Entendemos que, a fecha de hoy, el proceder de la mayor parte de los prestadores de servicios de la sociedad de la información, 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 los prestadores de servicios, 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 por medio de las *cookies* de rastreo –*tracking cookies*- que recopilan información sobre el comportamiento

de navegación de los individuos para ofrecer anuncios personalizados. Estas actuaciones pueden suponer violaciones de la privacidad. Por ello, el Grupo de Trabajo del Artículo 29, en un reciente dictamen (Dictamen 2/2010, de 22 de junio de 2010, sobre publicidad en línea basada en el comportamiento), entiende que, aunque se trata de prácticas que pueden aportar notables ventajas a la industria –y eventualmente a los usuarios-, comprometen la privacidad.

Por ello, lo más adecuado, para evitar tales infracciones de la privacidad, sería exigir, por ley y/o en virtud de la autorregulación, que, cuando se hiciera uso de tales técnicas, se informará explícitamente al consumidor de tal extremo a través de diversas medidas de carácter que son complementarias entre sí.

A tal efecto, podría exhibirse, como adelantamos, un icono interactivo suficientemente representativo –como se hizo en la industria norteamericana- así como indicar, antes de acceder a un sitio *Web* que hiciera uso de tal técnica, que el usuario va a acceder a "publicidad basada en el comportamiento".

También, con carácter adicional, podría desplegarse una ventana emergente en virtud de la que se informase sobre lo que tal práctica representa, a efectos de limitaciones de la privacidad, para el consumidor y/o usuario.

Por otro lado, si se optara por una autorregulación especialmente garantista con la privacidad, podría fijarse la necesidad de que los prestadores de servicios impusieran al usuario la necesidad de registrarse en los sitios *Web*. Naturalmente, estos últimos deberían, del mismo modo, permitir que los usuarios eliminasen la información que previamente han decidido conferir. Se trata del denominado derecho al olvido digital –o, en su equivalente anglosajón, *right be forgotten*-, especialmente visible en el ámbito de las redes sociales, los foros o las plataformas de vídeo, sin perjuicio de su relevancia en el ámbito de los buscadores.

Esta última facultad –el derecho al olvido- se alcanza en virtud de la cancelación de los datos personales, bien de oficio bien a instancia del interesado, una vez que ha transcurrido un determinado período de tiempo. Constituye un instrumento necesario para el efectivo cumplimiento del principio de finalidad que establece que los datos recogidos y registrados únicamente pueden emplearse según una finalidad concreta e implica la cancelación de los que ya no sean necesarios para la realización de la misma. Este derecho supone, además, que, transcurrido un concreto lapso de tiempo, ciertas informaciones deben ser eliminadas, ya que tiene por objeto contrarrestar uno de los riesgos más característicos del procesamiento informático de la información personal. Nos referimos a que se pueda recuperar, cuando un potencial interesado así lo considere, cualquier dato (por insignificante que este último pueda ser).

Estamos ante una materia sobre la que, a nivel europeo, se legislará en el año en curso para permitir que los usuarios de Internet tengan un control efectivo de sus datos. Ahora bien, aunque se modificara la legislación comunitaria o, en su caso, española, no sería suficiente por sí misma, dado que lo más adecuado sería impulsar la gestión de la huella digital. Esta última, como adelantamos, constituye el rastro que los usuarios van dejando a través de Internet. Lo más relevante pasa por que los usuarios estén adecuada y ampliamente informados sobre las potencialidades de la misma. A tal labor puede contribuir, de manera extraordinaria, los instrumentos derivados de la autorregulación, dado que una de sus funciones es la posibilidad de educar e informar al consumidor y/o usuario sobre los extremos que disciplina. En efecto, resulta de vital importancia que cada usuario –lo que es particularmente significativo para los menores de edad- sea consciente de qué información aporta y cuál es la política de privacidad de los sitios *Web* a los que accede.

Para, precisamente, poner fin a las actuaciones que, en ocasiones, conllevan las *cookies,* que, como hemos visto, comprometen la privacidad, la empresa de *softwareAdobeSystems* junto con los navegadores *Mozilla* y *Crome*, han ideado una interfaz de programación que permitirá eliminar, de manera permanente, tales archivos. Para ello, se utilizará una aplicación que se integrará en el panel de los navegadores.

Asimismo, los propios navegadores, de manera individual, están tomando cartas en

el asunto. En efecto, *Mozilla* opta por implantar un sistema en virtud del cual los propios usuarios podrían configurar su navegador de Internet, para, de esta manera, elegir si quieren o no recibir publicidad personalizada. La decisión por la que hubiera optado el usuario sería comunicada a los sitios *Web* y a los anunciantes a través de una cabecera HTTP "*Do NotTrack*". Por su parte, *Google* ha presentado una nueva propuesta para evitar el rastreo de los usuarios del navegador *Crome*. Se trata de una extensión, denominada "*KeepMyOpts-Out*", que permite al usuario dejar de recibir publicidad personalizada, de forma permanente, a través de las *cookies*. Finalmente, *Microsoft*, está trabajando para evitar este seguimiento en el navegador *Internet Explorer*, para lo cual se va a implementar un sistema de listas de protección contra rastreos -*Tracking ProtectionList*-. Ésta representa una herramienta similar al sistema *InPrivateSubscriptions* que se trató de incluir en *Internet Explorer* 8.0, si bien, finalmente, fue descartado por la oposición de los anunciantes.

En suma, de cuanto hemos enunciado, puede colegirse que los tres grandes navegadores enunciados (*Explorer* 9.0 –*Microsoft*-, Firefox –*Mozilla*- y *Crome* –*Google*-) han activado o tienen intención de poner en marcha medidas técnicas para impedir la entrada de *cookies* publicitarias en los ordenadores de los usuarios que así lo demanden. La puesta en práctica de tal medida –que se denomina *opt-out*- eliminará la posibilidad de recibir publicidad altamente personalizada. *A sensu contrario*, aunque la publicidad generalista en Internet continuará, se pondrá freno a las prácticas más invasivas. En todo caso, debe valorarse positivamente tales medidas acometidas por la propia industria. En virtud de las mismas, los propios navegadores refuerzan la protección de la privacidad de los usuarios. Repárese, en todo caso, que las mismas llegan después de que la *Federal TradeComission* (Comisión Federal de Comercio) haya recomendado la puesta en práctica de un mecanismo que evite el rastreo de los usuarios en Internet. A tal efecto, tal entidad, en diciembre de 2010, publicó un informe en el que se incluye un marco de recomendaciones para el gobierno, la industria y los legisladores. Debe hacerse notar que, en tal documento (Federal TradeComission, 2010), se dispone que la autorregulación sobre la cuestión que comentamos ha fallado a la hora de proveer una protección adecuada y significativa a los consumidores. Tales actuaciones, en todo caso, se suman a los deberes de carácter informativo a los que muy pronto, como hemos visto, se verán obligados los prestadores de servicios de la sociedad de la información sobre este particular.

Además de las medidas de carácter normativo mencionadas, no debe obviarse, insistimos, otras iniciativas fruto de la autorregulación –sin perjuicio de las que ya hemos comentado-, pues constituyen un sugerente complemento de aquéllas. Representan, en este sentido, un paradigma de referencia en la materia, al menos, las tres siguientes: 1. *EuropeanAdvertisingStandards Alliance* –EASA-, en octubre de 2008, aprobó *Digital MarketingCommunicationsBestPractice*, como instrumento de buenas prácticas susceptible de determinar el articulado de las regulaciones que se efectúen en la materia por los sistemas nacionales de autorregulación; 2. *InteractiveAdvertising Bureau Europe* –IAB Europe- elaboró, en mayo de 2009, *Social AdvertisingBestPractices* fundamentado en ciertos principios (IAB, 2009a); 3. y el documento de buenas prácticas –denominado *Global Principlesfor On-line BehavioralAdvertising*- ideado, en julio de 2009, por ciertas instituciones norteamericanas -en particular la *American Association of Advertising Agencies*, la *Association of NationalAdvertisers*, el *Council of Better Business Bureau*, la *Direct Marketing Association* y el *InteractiveAdvertising Bureau*- relativas a la publicidad comportamental (IAB, 2009b).

En definitiva, además del control externo que sobre este particular existe, lo más recomendable, a nuestro juicio, sería incentivar e implementar, a gran escala, el fenómeno de la autorregulación. En virtud de los compromisos asumidos voluntariamente, a tenor de esta última, debería informarse, de manera clara y visible, a los potenciales consumidores y/o usuarios sobre qué tipo de información se está recogiendo sobre los mismos, para qué y cuáles son las opciones de las que disponen

para evitar el rastreo de su comportamiento en la Red - se trata, en suma, de implementar la plena transparencia-.

BIBLIOGRAFÍA

ALPA, G. (1986) *Dirittoprivatodeiconsumi*, IlMulino, Bolonia.

ANSARI, A. y MELA, C. (2003) "E-customisation", *Journal of Marketing Research*, Vol. 40, núm. 2.

ARMSTRONG, S. (2002) *La publicidad en Internet. Cómo se transmite su mensaje a través de la World Wide Web,* Ediciones Deusto, Bilbao.

ASCARELLI, T. (1970) *Teoría de la concurrencia y de los bienes inmateriales*, Bosch, Barcelona.

AZLOR VILLA, A. (2001) "La estrategia en el e-business", *Boletín de Estudios Económicos*, Vol. 56, núm. 173.

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

BASSAT, L. (2003) *El libro rojo de la publicidad*, Barcelona.

BEATER, A. (2000) "ZumVerhältnis von europäischen und nationnalenWettbewerbsrecht (Überlegungen am beispiel des schutzesvorirreführenderwerbung und des verbraucherbegriffs)", *GRUR Int*.

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, núm. 3.

BENSOUSSAN, A. (1998) *Internet, aspectsjuridiques*, 2ª edición, Hermes, París.

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

BRUENING, P.J. y STEFFEN, M. (2004) "Spyware: Technologies, Issues, and Policy Proposals", *Journal of Internet Law*,Vol. 7, núm. 9.

CAMPUZANO TOMÉ, H. (2000) *Vida privada y datos personales*, Tecnos, Madrid.

CARVAJAL, F. y BARTHE, E. (2002) "Estrategia empresarial en Internet: Modelos de Negocio". En *Internet. Claves legales para la empresa*,Civitas y Accenture, Madrid.

CHECA GODOY, A. (2007) *Historia de la publicidad*, NetBiblo, La Coruña.

CHITTENDEN, L. y RETTIE, R. (2003) "An evaluation of *email* marketing and factors affecting response", *Journal of Targeting, Measurements and Analysis for Marketing*, Vol. 11, núm. 3.

CLARKE, R. (1994) "Computer Matching by Government Agencies:The Failure of Cost/Benefit Analysis as a Control Mechanism", *Information Infrastructure & Policy*, Vol. 4, núm. 1.

CORREDOIRA y ALFONSO, L. (1994) *Derecho de la información (II). Los mensajes informativos*,Colex, Madrid.

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

D´ORAZIO, R. (1999) "Datipersonali in rete aperta". En CUFFARO, V. y RICCIUTO, V. (Eds.), *Iltratamentodeidatipersonali*, Vol. 2, Giappichelli, Torino.

DOMÍNGUEZ PÉREZ, E.M. (1999) "La alegación publicitaria redactada en términos superlativos. La exageración publicitaria", *Estudios sobre Consumo*, núm. 48.

FARRÉ LÓPEZ, P. (2003) "El derecho de rectificación en el ámbito de la

publicidad comercial". En *Homenaje a Luis Rojo Ajuria: escritos jurídicos*, Universidad de Cantabria, Santander.

FEDERAL TRADE COMISSION (2010) "Do Not Track", http://www.ftc.gov/os/testimony/101202donottrack.pdf.

FERRER, C.G. (2001) *La publicidad en Internet*, Edimarco, Madrid.

FLETCHER, K. WHEELER, C. y WRIGHT, J. (1991) "Database marketing: a channel, a medium or a strategic approach?",*European Journal of Marketing*, Vol. 10, núm. 2.

FONT GALÁN, J.I. (1987) *Constitución económica y derecho de la competencia*, Tecnos, Madrid.

FONT GALÁN, J.I. (1990) "El tratamiento jurídico de la publicidad en la Ley General para la Defensa de los Consumidores y Usuarios". En *Curso sobre el nuevo Derecho del consumidor*, Ministerio de Sanidad y Consumo, Instituto Nacional de Consumo.

FORD, R.T. (2000) "Save the Robots: Cyber Profiling and Your So-Called Life", *Stanford Law Review*, Vol. 52, núm. 5.

GARCÍA UCEDA, M. (2001) *Las claves de la publicidad*, 6ª ed., Esic, Madrid.

GHIDINI, G. (1968) *Introduzione allo studio de lla pubblicitá comerciale*, Giuffrè, Milán.

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

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. (2009) "Las comunicaciones comerciales en el marco de la contratación electrónica". En ORDUÑA MORENO, J. y AGUILERA ANEGÓN, G. (Dirs.), y PLAZA PENADÉS, J. y BALLUGUERA GÓMEZ, C. (Coords.), *Comercio, administración y registro electrónicos*, Thomson Reuters, Navarra.

HAAN, S.C. (2000) "The persuasion route of the Law: advertising and legal persuasion", *Columbia Law Review*, Vol. 100, núm. 5.

HALL, M. (1997) "Four models on how advertising works", *Commercial Communications. The Journal of Advertising and Marketing Policy and Practice in the European Community*, núm. 9.

HAND, D.J. (1998) "Data Mining: Statistics and more?",*The American Statistician*, Vol. 52, núm. 2.

HARDING, W.T. REED, A.J. y GRAY, R.L. (2001) "Cookies and Web Bugs: What They are and How They Work Together", *Information Systems Management*, Vol. 18, núm. 3.

HERRERO-TEJEDOR ALGAR, F. (1998) "La protección del honor y la intimidad en el ámbito de las telecomunicaciones". En MERINO MERCHAN, J.F. y PÉREZ-UGENA COROMINA, M. (Coords.), *Régimen de las telecomunicaciones*, Tecnos, Madrid.

IAB (2009a) "Social Advertising Best Practices", http://www.iab.net/media/file/Social-Advertising-Best-Practices-0509.pdf.

IAB (2009b) "Self-regulatory principles for On-line Behavioral Advertising", http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

JANCZEWSKI, L.J. y 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, núm. 1-2.

JUILIÁ BARCELÓ, R. (2000) "Cookies,perfiles, direcciones IP: cuestiones pendientes en la legislación sobre protección de datos", *Novática*, núm. 148.

KAYE, B.K. y MEDOFF, N. (2001) *Just A Click Away: Advertising on the Internet*,Allyn and Bacon, Massachusetts.

KLANG, M. (2003) "Spyware: Paying for Software With our Privacy", *International Review of Law Computers & Technology*, Vol. 17, núm. 3.

KUSSMAUL, W. (2007) *Own Your Privacy: Privacy and Security Are Not Antithetical*, PKI Press.

LAVILLA RASO, M. (2002) *Actividad publicitaria en Internet*, Rama, Madrid.

LEVINE, J.R. y 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.

LÓPEZ DE AGUILETA, C. y TORRES ROMAY, E. (2007) "Medios y soportes alternativos para una publicidad convencional: publicidad "off the line", *Pensar la Publicidad*, Vol. 1, núm. 2.

LÓPEZ LITA, R. (2004) *La publicidad local*, Publicaciones de la Universidad Jaime I, Castellón de la Plana.

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. y ALSAID, A. (2003) "**Hidden surveillance by Web sites: Web bugs in contemporary use** , *Communication of the ACM*, Vol. 46, núm. 12.

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

MEEKER, M. (2001) *La publicidad en Internet*, Granica, Barcelona.

MENA, J. (1999) *Data Mining your website*, Digital Press, Boston.

MÉNDIZ NOGUERO, A. (2000) *Nuevas formas publicitarias: patrocinio, productplacement, publicidad e Internet*, Universidad de Málaga, Málaga.

MITJANS PERELLÓ, E. (2009) "Impacto de las redes sociales en el derecho a la protección de datos personales", *Anuario de la Facultad de Derecho de la Universidad de Alcalá de Henares*, Vol. 2.

MORALES MORENO, A.M. (1988) "Información publicitaria y protección del consumidor (Reflexiones sobre el art. 8 de la LGCU)". En *Homenaje a Juan BerchmansVallet de Goytisolo*, Vol. VIII, Consejo General del Notariado, Madrid.

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

MUÑOZ MACHADO, S. (1994) "Advertising in the Spanish Constitution". En SKOURIS, W. (Ed.), *Advertising and Constitutional Rights in Europe: A study in comparative constitutional law* (GebundeneAusgabe), NomosVerlagsgesellschaft, Baden-Baden.

NABBALI, T. y PERRY, M. (2003) "Going for the **throat**: Carnivore in an Echelon World - Part I", *Computer Law and Security Report*, Vol. 16, núm. 9.

NGAI, E.W. y WAT, F.K. (2001) "A Literature Review and Classification of Electronic Commerce Research", *Information and Management*, núm. 39.

NIVARRA, L. y RICCIUTO, V. (2002) *Internet e ildirittodeiprivati. Persona e proprietà intellettual enelleretitelematiche*, Torino.

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, núm. 1.

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 UniversitatOberta de Catalunya, Barcelona.

PEPPERS, D. y ROGERS, M. (1999) *The One to One Manager*, Doubleday, New York.

PERLADO LAMO DE ESPINOSA, M. (2006) *Planificación de medios de comunicación de masas*, Mc Graw Hill, Madrid.

PINO ABAD, M. (1991) *La disciplina jurídica en la actividad publicitaria en la Ley de publicidad de 1988*, Ministerio de Sanidad y Consumo, Madrid.

PLAZA PENADÉS, J. (2007) "Aspectos básicos de la protección de datos de carácter personal". En DE VERDA y VEAMONTE, J.R. (Coord.), *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, Thomson Aranzadi, Navarra.

QUALTER, T.H. (1994) *Publicidad y democracia en la sociedad de masas*, Paidos Ibérica, Barcelona.

RADCLIFF, D. (2004) "Spyware", *Network World*,Vol. 21, núm. 4.

RAMONET, I. (2002) *La post-televisión: multimedia, Internet y globalización económica*, Icaria, Barcelona.

ROMERO CALMACHE, M. y BANJUL PEYRÓ, C. (2010) "La publicidad en la era digital: el microsite como factor estratégico de las campañas publicitarias on-line", *Comunicar*, núm. 34.

SAN MARTÍN GUTIÉRREZ, S. y LÓPEZ CATALÁN, B. (2010) "Posibilidades de la compraventa B2C por teléfono móvil en comparación con Internet", *Cuadernos de Gestión*, Vol. 10, núm. 1.

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

SHARMA, A. y SHET, J. (2004) "Web based marketing the coming revolution in marketing thought and strategy", *Journal of Business Research*, núm. 57.

SPANG, K. (2005) *Persuasión. Fundamentos de retórica*, Eunsa, Pamplona.

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

STAZI, A. (2004) *La pubblicitàcommerciale on line*, GiuffrèEditore, Milano.

SUÁREZ VILLEGAS, J.C. y PÉREZ CHICA, M.A. (2002) *La publicidad al desnudo*, Editorial Mad, Sevilla.

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

URBACH, R.R. y KIBEL, G.A. (2004) "Adware/ Spyware: An Update Regarding Pending Litigation and Legislation", *Intellectual Property & Technology Law Journal*, Vol. 16, núm. 7.

VICENTI, M. (2003) *Manuale del diritto di Internet della disciplina della firma elettronica*, La Tribuna, Piacenza.

VOLKMER, C.J (2004) "Should Adware and Spyware Prompt Congressional Action?",*Journal of Internet Law*, Vol. 7, núm. 11.

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