Revista de Estudios Económicos y Empresariales
Núm. 22, 2010, pp. 101-134 - ISSN: 0212-7237

NUEVAS COORDENADAS EN EL ÁMBITO DE LA WEB 2.0: EL CASO DE LA PUBLICIDAD COMPORTAMENTAL

Por
DAVID LÓPEZ JIMÉNEZ
Becario de investigación del Ministerio de Educación y Ciencia
Programa FPU
FRANCISCO JOSÉ MARTÍNEZ LÓPEZ
Catedrático y Rector de la Universidad de Huelva

RESUMEN:

Una reciente modalidad publicitaria que está protagonizando un notable éxito en Internet es la publicidad comportamental. Aunque puede suponer ciertas ventajas para las empresas y los usuarios, no está exenta de riesgos sobre todo en materia de privacidad. Para, precisamente, proteger al consumidor y/o usuario en esta novedosa faceta de la Web 2.0 se han aprobado un elenco de normas legales complementadas por el sugerente fenómeno de la autorregulación.

Palabras clave: autorregulación; interactividad; privacidad; publicidad comportamental; Web 2.0.

ABSTRACT:

A new mode of advertising, behavioural advertising, is enjoying considerable success on the Internet. But the advantages for companies and users are weighed against the risks to privacy. A range of legal norms have been approved to complement self-regulation in order to protect the consumer and / or user of this new facet of Web 2.0.

Keywords: self-regulation; interactivity; privacy; behavioral targeting; Web 2.0.

1. INTRODUCCIÓN

La *Web* 2.0 representa un novedoso espacio en el que tanto las empresas como los consumidores tienen diversas formas de interactuar. Sin embargo, no es un escenario estático sino, más bien, todo lo contrario, dado que está en permanente y vertiginoso cambio. En este último sentido, destaca la denominada publicidad comportamental.

En el tema que nos ocupa hemos pasado por varias etapas. *Grosso modo*, podríamos, al menos, diferenciar dos grandes fases. Una primera en la que la fórmula en la que las empresas se han dejado ver en la Red ha sido a través de la búsqueda de contenidos y de información relevante por parte de los usuarios. En este momento, los buscadores desempeñaban un papel prioritario. Posteriormente, se pasa a un segundo período en el que, siendo todavía visible la posición de preeminencia de los buscadores, tanto las empresas como los consumidores interactúan activamente en espacios adicionales. Existen numerosos servicios que,

en cierta medida, están modificando las reglas de juego. A este respecto, cabe referirse al destacado papel que, entre otros, están desarrollando las redes sociales, los *blogs* y los foros.

Cuando el usuario recurre a Internet con la finalidad de informarse y, en su caso, contratar un determinado bien y/o servicio puede, de manera consciente, realizar múltiples actividades cual, por ejemplo, podría ser acceder a ciertos sitios *Web*, formular preguntas en un determinado foro, comentarios en un *blog* y adherirse a un perfil corporativo de una red social. En todo caso, el uso que cotidianamente realiza el usuario de la red de redes, sin que este último lo sepa ni mucho menos lo autorice, puede ser rastreado, con fines de carácter comercial, para remitirle publicidad que, dado que estará adaptada a sus preferencias, será de su interés. En otros términos, la publicidad basada en comportamiento analiza y utiliza la información de los hábitos de los usuarios en Internet para elaborar un perfil detallado con el objetivo de ofrecer publicidad segmentada acorde a las preferencias y datos de estos perfiles.

La recopilación de datos relativos a la actividad de los usuarios fundamentados en la navegación por Internet puede proporcionar una imagen detallada de la vida de los mismos, lo cual puede suponer una vulneración de la privacidad. Aunque la publicidad comportamental puede aportar ciertas ventajas tanto a la industria como al usuario, debe valorarse la invasión de la privacidad que tal forma publicitaria puede representar.

Existen un creciente número de mecanismos técnicos –como, entre otros, las *cookies*, *spyware*, troyanos y *web bugs*- que, entre otros fines, han sido concebidos para realizar la monitorización del comportamiento del usuario en cuyo dispositivo se instalan. Ahora bien, hay ciertos límites establecidos por la legislación actual que, dicho sea de paso, se verán reforzados, a tenor de una reciente modificación, en los próximos años. No debe olvidarse prácticas que pueden resultar censurables, de nuevo por el quebranto que pueden suponer en la protección de datos de carácter personal, como es la lectura, por parte de terceros, del contenido de los correos electrónicos enviados y/o recibidos para ofrecer publicidad, directa o indirectamente, vinculada a los mismos. Finalmente, se ha puesto vigorosamente en práctica el fenómeno de la geolocalización con especial proyección de futuro en el caso de las redes sociales.

El ordenamiento jurídico no debe, en absoluto, permitir que la aplicación de las nuevas tecnologías suponga para el usuario un menoscabo de sus derechos de carácter fundamental. Con buen criterio, el legislador comunitario y europeo, a

través de la normativa legal, tratan de imponer ciertas restricciones a las prácticas mencionadas, si bien, con carácter complementario, se fomenta el recurso a la autorregulación de la industria. Esta última debe coadyuvar a elevar el nivel de protección establecido en la legislación.

2. LA WEB 2.0 CON FINES COMERCIALES: ESTADO ACTUAL Y PERSPECTIVAS DE FUTURO

La irrupción de las nuevas tecnologías de marcado carácter social –*blogs*, *wikis*, *podcast*, redes sociales, etc.- ha determinado un alto grado de interconectividad entre los usuarios de Internet, lo que, dicho sea de paso, les permite intercambiar todo tipo de opiniones sobre diferentes productos y experiencias con otras personas[1]. La llegada de la *Web* 2.0 ha supuesto una revolución, pues el potencial usuario adquiere un nuevo papel dentro del soporte, ya que deja de ser un mero espectador de contenidos –que, en cierta medida, acontecía en la *Web* 1.0-, para ser el que elige, el que participa e, incluso, el que crea esos contenidos. En suma, la *Web* 2.0 es una *Web* más colaborativa que permite a sus usuarios acceder y participar en la creación de un conocimiento ilimitado y, como consecuencia de esta interacción, se generan nuevas oportunidades de negocio para las empresas[2].

En este último sentido, la *Web* 2.0 ha modificado, de forma sustancial, con respecto a hace relativamente poco, la forma en la que las empresas se dirigen a sus potenciales clientes. Cada vez un mayor número de las mismas recurren con fines publicitarios a las novedosas manifestaciones de la *Web* 2.0, para, precisamente, captar consumidores, fidelizarlos, y, en definitiva, para vender más con una inversión publicitaria más personalizada. De hecho, según pone de manifiesto el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información en 2009[3], el 70% de la población española consume contenidos

[1] RALLO LOMBARTE, A. (2009) "La protección de datos en España", *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, Vol. 2, p. 24.

[2] BARRIUSO RUIZ, C. (2009) "Las redes sociales y la protección de datos hoy", *Anuario de la Facultad de Derecho de la Universidad de Alcalá de Henares*, Vol. 2, p. 306; 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, p. 129.

[3] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (2009) *Informe anual de los contenidos digitales en España 2009*, Ministerio de Industria, Turismo y Comercio, Madrid.

digitales –debiéndose entender, naturalmente, incluida la publicidad-. En línea con la apreciación realizada, cabe indicar que 24,3 millones de españoles de más de 10 años –o, lo que es lo mismo, el 60,4% de la población- hacen uso de Internet. La comunidad de internautas españoles es, dicho sea de paso, la más activa del mundo en el uso de las redes sociales tras Brasil.

Debe tomarse conciencia de que la publicidad virtual representa un mercado en continuo crecimiento. A pesar de la fuerte crisis económica, que desde hace unos años sufrimos, la inversión publicitaria en Internet no ha dejado de crecer, siendo, asimismo, las previsiones de futuro al respecto muy optimistas.

La inversión real estimada en publicidad en medios convencionales alcanzó los 5.621,3 millones de euros durante el año 2009, cifra que supone un decrecimiento del 20,9% respecto a la registrada en el año anterior. Por segundo año consecutivo –desde 2008-, todos los medios presentan caídas en la cifra de negocio con la única excepción de Internet. Este último ha tenido un crecimiento interanual de 7,2%, llegando a obtener un volumen de inversión publicitaria de 654,1 millones de euros frente a los 610,0 millones del año 2008. El porcentaje que Internet supone sobre el total de la inversión en el año 2009 es del 11,6%. Como anticipamos, diversos estudios operados por entidades de renombre en la materia[4] prevén un incremento significativo de la publicidad en Internet para los próximos años. En este último sentido, entre los instrumentos que contribuirán al importante crecimiento de la publicidad interactiva ocupan un destacado lugar los *smartphones*[5] o teléfonos inteligentes que cada vez reúnen más caracteres propios de los ordenadores personales.

A propósito de este último particular, el volumen de mercado del marketing móvil en España, según el estudio operado por Accenture y MMA Spain[6], se prevé que supere los 100 millones de euros en 2010 y los 240 millones en 2012, lo que supone un 70% de crecimiento medio anual. Además, se estima que, en

[4] MEDIA SCOPE (2009) "El Estudio de Calidad de los Medios de Comunicación en España", http://www.grupoconsultores.com/spa/files/mediascope09.pdf; PRICEWATERHOUSECOOPERS (2009) "Global Entertainment and Media Outlook: 2009-2013", http://kc3.pwc.es; ARCEMEDIA (2010) "Índice de inversión publicitaria", http://www.arcemedia.es/images/i2p_1_2010.pdf.

[5] GERON, G. (2010) "Business Aspects of the Internet of Things: Mobile Marketing". En MICHAHELLES, F. (Ed.), *Business Aspects of the Internet of Things, Seminar of Advanced Topics*, ETH, Zurich, pp. 39-44.

[6] ACCENTURE y MMA SPAIN (2009) "I Estudio de Inversión en Marketing y Publicidad Móvil. El sector en cifras", http://www.puromarketing.com/files/mma-estudio-marketing-movil.pdf.

menos de 10 años, haya más accesos a Internet desde dispositivos móviles que desde el propio ordenador. La tecnología móvil se ha convertido, por consiguiente, en un paradigma de la convergencia de diversos canales y está suponiendo una auténtica revolución.

En todo caso, el crecimiento que, en los últimos años, protagoniza Internet se ve acompañado, lo que es un plus muy relevante, de un mayor consumo de tal canal. En efecto, como pone de relieve la Asociación Europea de Publicidad Interactiva (2010)[7], el consumo actual de la Red es superior al de la televisión. La innovación tecnológica junto con las numerosas opciones que tienen los usuarios para conectarse a la Red han conseguido aumentar significativamente el uso de Internet en España hasta las 13,6 horas semanales, frente a las 13 horas que se dedican a la televisión. Esta cifra sitúa a España, además, como el quinto país europeo con mayor consumo de Internet. Todo parece indicar que, a pesar de su extraordinaria juventud, la publicidad virtual protagonizará un notable incremento frente a los restantes medios.

Aunque, como veremos, la publicidad *online* presenta numerosas ventajas para las empresas y, en su caso, para los consumidores, no está exenta de eventuales vulneraciones de la privacidad de los usuarios. En efecto, las empresas recurren en Internet a técnicas de monitorización de los usuarios con fines publicitarios que se fundamentan en su comportamiento durante la navegación. El elenco de prácticas no siempre conocidas –ni consentidas- por el potencial usuario, pueden pasar totalmente desapercibidas –como, por ejemplo, las *cookies flash*, las *cookies* de rastreo tradicionales u otros instrumentos como los *spyware*-, pues se sirven de un rastreo –insistimos que invisible para su titular- de las actuaciones electrónicas realizadas. Como posteriormente veremos, tal proceder puede suponer una invasión de la privacidad, por lo que el legislador establece, con buen criterio, ciertos límites.

Pero no todas las acciones desarrolladas por las empresas con fines comerciales pueden tener su origen en hechos totalmente desapercibidos para el usuario. En efecto, cada vez en mayor medida, estos últimos pueden efectuar ciertas valoraciones en las redes sociales (incluyendo, en este sentido, la información reflejada en el perfil), o actos dirigidos a expresar el interés por una determinada empresa, bien o servicio –como la activación de la casilla "Me gusta" en *Facebook*

[7] ASOCIACIÓN EUROPEA DE PUBLICIDAD INTERACTIVA (2010) "Estudio Mediascope Europe 2010", http://recursos.anuncios.com/files/340/66.pdf.

o *retweet* de *Twitter*- que las empresas pueden tener en cuenta en sus campañas comerciales. Asimismo, cabe poner de relieve que un elevado número de sitios *Web* de empresas están optando por añadir iconos para que los usuarios puedan interactuar desde el perfil de su red social para que, precisamente, los contenidos se compartan más. También pueden, indudablemente, realizar comentarios –de carácter positivo o negativo-, en *blogs*, foros o sitios *Web* especializados sobre opiniones.

Pero el carácter abierto de las redes sociales ha configurado una nueva y prometedora realidad en la que tienen cabida no sólo las personas, sino también las empresas, que buscan en ellas un potente escaparate de carácter publicitario. Conviene también incidir en que los avances que las redes sociales y las plataformas colaborativas suponen están modificando las prácticas comerciales[8], redefiniendo, de esta manera, la forma electrónica de ofertar bienes y servicios, a través de la publicidad hipercontextualizada, según los perfiles de usuario, diversificando el mercado y creando nuevos canales de comunicación. Los *spammers* pueden utilizar la información personal disponible en las redes sociales para recopilar direcciones de correo electrónico de modo que, cuando envíen *spam*, parezca que se envía desde los contactos directos. Debe precisarse que un correo electrónico recibido desde una dirección de un contacto, es mucho más probable que llegue a abrirse, pues parecerá, por decirlo en términos coloquiales, un correo "más fiable". Además, el *spammer* recogerá información relativa a aficiones o intereses con el fin de crear mensajes con temas de interés para el usuario, lo que, unido a que se recibe de un contacto, aumentará las posibilidades de que el usuario abra ese correo malicioso y que el *malware* que, en su caso, contenga, se active.

En otras palabras, la *Web* 2.0 en general y las redes sociales en particular, se erigen en una poderosa herramienta de marketing para las empresas a la hora de promocionar sus productos y servicios ganando cada vez más terreno. Estos nuevos

[8] En este sentido, no resulta lícito el recurso a técnicas comerciales, como el *spam*, claramente vulneradoras de la privacidad. Así, a título de ejemplo, cabe referirse al caso en el que en 2008 una persona fue multada por un juez estadounidense a pagar más de 873 millones de dólares –unos 697 millones de euros- por mandar, a través de la red social *Facebook*, correos electrónicos no solicitados relativos a temas de orientación sexual, ofertas no solicitadas de medicamentos y otros productos. La imposición de la multa se efectuó en virtud de la Ley de Control de Pornografía y Marketing No Solicitados - *Controlling the Assault of Non-Solicited Pornography and Marketing Act*-. La sanción no cabe duda que tendrá un importante efecto disuasorio de cara a posibles infractores futuros de la norma mencionada.

modelos de negocio basados en el comercio electrónico pueden dar origen a un cierto grado de incertidumbre en el usuario sobre todo respecto a, entre otras cuestiones, la aludida privacidad[9], la seguridad de las transacciones electrónicas, el perfeccionamiento y validez de los contratos o a la normativa aplicable o jurisdicción competente en caso de litigio.

3. LA PUBLICIDAD COMPORTAMENTAL: APRECIACIONES DESDE LA EVENTUAL VIOLACIÓN DE LA PRIVACIDAD

3.1. TÉCNICAS DE MONITORIZACIÓN DEL COMPORTAMIENTO FUNDAMENTADAS EN LA NAVEGACIÓN

Los datos de carácter personal, en la actualidad, tienen un extraordinario valor[10]. En este sentido, los perfiles constituidos se compran y se venden a un precio nada desdeñable[11] y, lo peor de todo, se trata de una actividad invasiva de nuestra intimidad[12], pues, en muchas ocasiones, no habrá resultado, en absoluto, conocida ni, mucho menos, consentida[13]. De hecho, existen numerosos

[9] Sobre la privacidad en sentido amplio, recomendamos la consulta de VEGA VEGA, J.A. (2004) "Protección de datos de carácter personal en el comercio electrónico", *Revista de Estudios Económicos y Empresariales*, núm. 16, pp. 147-192; VEGA VEGA, J.A. (2005) *Contratos electrónicos y protección de los consumidores*, Reus, Madrid, pp. 357-400.

[10] 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, pp. 85-118.

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

[12] NGAI, E. W. y WAT, F. K. (2001) "A Literature Review and Classification of Electronic Commerce Research", *Information and Management*, núm. 39, pp. 415-419; 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, pp. 201-235; SHARMA, A. y SHET, J. (2004) "Web based marketing the comino revolution in marketing thought and strategy", *Journal of Business Research*, núm. 57, pp. 696-702.

[13] JUILIÁ BARCELÓ, R. (2000) "Cookies, perfiles, direcciones IP: cuestiones pendientes en la legislación sobre protección de datos", *Novática*, núm. 148, pp. 20-23; SERRA RODRÍGUEZ, A. (2000) "Los derechos de los particulares en la nueva Ley de protección de datos de carácter personal", *La Ley*, Vol. 6, www.laley.net; LLÁCER MATACÁS, M. R. (2003) "La protección de los datos personales en Internet". En BARRAL VIÑALS, I. (Coord.), *La regulación del comercio electrónico*,

mecanismos tecnológicos ideados para tal fin[14] cuales, 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[15].

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[16],

---

Dykinson, Madrid, pp. 157-190; JAWAHITHA, S. (2004) "Consumer protection in E-commerce: Analyzing the Statutes in Malasya", *Journal of American Academy of Business*, Vol. 4, núm. 1-2; VEGA VEGA, J.A. (2005) *Contratos electrónicos y...*, cit., pp. 168 y 358.

[14] BENSOUSSAN, A. (1998) *Internet, aspects juridiques*, 2ª edición, Hermes, París; 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*, núm. 3, pp. 173-178; SCHWARTZ, P. M. (2004) "Property privacy and personal data", *Harvard Law Review*, Vol. 117, pp. 2055-2128; VEGA VEGA, J. A. (2006) "La publicidad comercial y los consumidores", *Revista de Estudios Económicos y Empresariales*, núm. 18, pp. 94 y 95; MARTÍNEZ MARTÍNEZ, M. FERNÁNDEZ RODRÍGUEZ, F. y SACO VÁZQUEZ, M. (2008) *Supermercados.com. Marketing para los supermercados virtuales*, Esic, Madrid.

[15] No resulta necesario celebrar electrónicamente un contrato para que se aporten datos personales. Es suficiente con comenzar a navegar por Internet para que se aporten datos personales. Sobre este extremo recomendamos la lectura de RICO CARRILLO, M. (2003) *Comercio electrónico, Internet y Derecho*, Legis, Caracas, pp. 217-218; GUILLÉN CATALÁN, R. (2005) *Comunicaciones comerciales no solicitadas*, Thomson Aranzadi, Navarra, p. 54; 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, p. 286; MITJANS PERELLÓ, E. (2009) "Impacto de las redes sociales...", cit., p. 115.

[16] Así, 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. Sobre este particular, entre otros, 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, pp. 456-467; KUSSMAUL, W. (2007) *Own Your Privacy: Privacy and Security Are Not Antithetical*, PKI Press, p. 26; GOLUMBIC, M. C. (2008) *Fighting terror online: the convergence of security, technology, and the law*, Springer, p. 153; JANCZEWSKI, L. J. y COLARIK, A. (2008) *Cyber warfare and cyber terrorism*, Idea Group, p. 309.

si bien nos centraremos en aquél aspecto por ser el que más interesa a efectos del presente trabajo.

El potencial de esta información es enorme[17], 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[18], 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[19]. 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[20]. La *cookie* está formada por el nombre del usuario configurado en el navegador, seguido del símbolo arroba (@), y el nombre del servidor que

[17] RIBAS ALEJANDRO, X. (1999) "Marketing y publicidad en Internet", *Revista Autocontrol de la Publicidad*, núm. 28; 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. y BATUECAS CALETRÍO, A. (Coords.), *Autores, consumidores y comercio electrónico*, Colex y Caja Duero, Madrid, pp. 235-249; 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.

[18] Sobre esta cuestión nos remitimos al trabajo de VEGA VEGA, J. A. (2003) "Comunicaciones comerciales por vía electrónica", *Revista General de Legislación y Jurisprudencia*, núm. 4, pp. 615-638.

[19] WENZ, C. (2001) *Active Server Pages*, Marcombo, p. 173; BASKIN, B. y PILTZECKER, T. (2006) *Combating spyware in the enterprise*, Syngress, p. 22; TREESE, G.W. y STEWART, L.C. (2003) *Designing systems for Internet commerce*, Addison-Wesley, p. 80; GUTIÉRREZ GONZÁLEZ, P.P. PEDREIRA SÁNCHEZ, D. y VELO MIRANDA, M. (2005) *Diccionario de la publicidad*, Editorial Complutense, Madrid, p. 316; CROLL, A. y POWER, S. (2009) *Complete web monitoring*, O'Reilly Media, p. 77; LEVINE, J. R. y LEVINE, M. (2010) *The Internet For Dummies*, 12ª ed., Wiley Publishing, Indiana, p. 24.

[20] 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, pp. 271-280; ERDOZÁIN LÓPEZ, J. C. (2007) "La protección de los datos de carácter personal en las telecomunicaciones", *Aranzadi Civil*, núm. 2, pp. 1845-1889.

envía la *cookie*, más la extensión "txt" que la identifica como fichero de texto[21]. El potencial de esta información, a efectos de marketing, es enorme[22].

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 *flash* –llamadas también *supercookies*-. A título anecdótico, diremos que pueden almacenar 25 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*

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

[22] RIBAS ALEJANDRO, X. (1999) "Marketing y publicidad en Internet", *Revista Autocontrol de la Publicidad*, núm. 28; 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. y BATUECAS CALETRÍO, A. (Coords.), *Autores, consumidores y comercio electrónico*, Colex y Caja Duero, Madrid, pp. 235-249; 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.

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 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 práctica se conoce como *respawning*.

En cuanto a los troyanos –como los *trap doors*[23], *logic bombs*[24] y *data diddling*[25], 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[26].

Los *spyware*[27] son programas espía que monitorizan el comportamiento de los consumidores y, adicionalmente, ocasionan fallos en el rendimiento y estabilidad de los ordenadores. Podemos diferenciar tres grandes tipos de *spyware*: 1) el

[23] Las puertas falsas *-trap doors-* 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.

[24] Las bombas lógicas *–logic bombs-* 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*.

[25] La modificación de datos *-data diddling* o *tampering-* se refiere a la alteración desautorizada a los datos o del *software* del sistema, incluyendo borrado de archivos.

[26] VELÁZQUEZ BAUTISTA, R. (2001) *Derecho de Tecnologías de la información y las comunicaciones (T.I.C.)*, Colex, Madrid; 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; VÁZQUEZ RUANO, T. (2007) "La seguridad electrónica en la fase precontractual. Un apunte desde el derecho comunitario". En MADRID PARRA, A. (Dir.), y GUERRERO LEBRÓN, M. J. (Coord.), *Derecho Patrimonial y Tecnología. Revisión de los principios de la contratación electrónica con motivo del Convenio de las Naciones Unidad sobre Contratación Electrónica de 23 de noviembre de 2005 y de las últimas novedades legislativas*, Marcial Pons, Madrid-Barcelona, pp. 251-274.

[27] Sobre este extremo pueden verse, entre otros, KLANG, M. (2003) "Spyware: Paying for Software With our Privacy", *International Review of Law Computers & Technology*, Vol. 17, núm. 3, pp. 313-322; SCHULTZ, E. (2003) "Pandora's Box: Spyware, Adware, Autoexecution, and NGSCB", *Computers & Security*, Vol. 22, núm. 5, p. 366; BRUENING, P. J. y STEFFEN, M. (2004) "Spyware: Technologies, Issues, and Policy Proposals", *Journal of Internet Law*, Vol. 7, núm. 9, pp. 3-8; RADCLIFF, D. (2004) "Spyware", *Network World*, Vol. 21, núm. 4, p. 51; STAFFORD, T. F. y URBACZEWSKI, A. (2004) "Spyware: the ghost in the machine", *Communications of the Association for Information Systems*, Vol. 14,

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[28].

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[29]. 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[30]. 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[31]. 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

pp. 291-306; 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, pp. 12-16; VOLKMER, C.J (2004) "Should Adware and Spyware Prompt Congressional Action?", *Journal of Internet Law*, Vol. 7, núm. 11, pp. 1-8; SIPIOR, J.C. WARD, B.T. y ROSELLI, G.R. (2005) "The Ethical and Legal Concerns of Spyware", *Information Systems Management*, Vol. 22, núm. 2, pp. 39-49.

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

[29] 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, pp. 258-264.

[30] 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, pp. 197-210.

[31] 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, pp. 17-24.

predeterminado o los valores de *cookies*. De esta manera, se recogen numerosos datos estadísticos y se consigue efectuar el seguimiento de los usuarios[32].

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.

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[33]. 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 solo a las *cookies* sino también a cualquier otra tecnología utilizada para almacenar 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, por un lado, hay que facilitar a los usuarios de Internet información clara y completa, en particular sobre los fines del tratamiento

[32] PAYERAS CAPELLA, M. M. y 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.

[33] VÁZQUEZ RUANO, T. (2002) "Aproximación jurídica al *Spam* desde la protección de datos de carácter personal", *Revista de la Contratación Electrónica*, núm. 33, p. 20.

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. 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. 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[34].

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

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

–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[35], en particular sobre los fines del tratamiento de los datos". 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[36].

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 estos 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

[35] 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.

[36] 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.

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 estas 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 solo del hecho 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 un reciente dictamen[37], entiende que, aunque se trata de herramientas que pueden aportar notables ventajas a la industria –y eventualmente a los usuarios-, comprometen la privacidad.

Además de las medidas de carácter normativo mencionadas, no debe obviarse las iniciativas fruto de la autorregulación, pues constituyen un sugerente complemento de aquéllas. Representan, en este sentido, un paradigma de referencia en la materia, al menos, las tres siguientes: 1. la *European Advertising Standards Alliance* –EASA-, en octubre de 2008, aprobó *Digital Marketing Communications Best Practice*, 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. *Interactive Advertising Bureau Europe* –IAB Europe- elaboró, en mayo de 2009, *Social Advertising Best Practices* fundamentado en ciertos principios[38]; 3. el documento de buenas prácticas –denominado *Global Principles for Online Behavioral Advertising*- elaborado, en julio de 2009, por ciertas instituciones norteamericanas -en particular la *American*

[37] Se trata del Dictamen 2/2010, de 22 de junio de 2010, sobre publicidad en línea basada en el comportamiento, disponible en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf.

[38] Puede verse en http://www.iab.net/media/file/Social-Advertising-Best-Practices-0509.pdf.

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[39]. Resulta conveniente que las prácticas mencionadas en estos documentos inspirasen los sistemas nacionales de autorregulación. Por su importancia, nos referiremos a los dos últimos que hemos mencionado.

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 tercer 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

[39] Nos referimos al denominado *Self-regulatory principles for Online Behavioral Advertising*, para cuya consulta recomendamos: http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

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.

3.2. LECTURA INCONSENTIDA DE CORREOS ELECTRÓNICOS, POR TERCEROS, CON FINES PUBLICITARIOS: EL CASO DE GMAIL

Es patente la enorme importancia, por el volumen de los datos que se tratan y por las características de estos tratamientos, de los servicios de búsqueda en Internet -los habitualmente denominados buscadores-, cuya función principal se centra en ofrecer índices de resultados relativos a una búsqueda, como direcciones y archivos almacenados en servidores *Web*, a través de la introducción de palabras clave[40], ordenando, de este modo, toda la información disponible en Internet, haciéndola más accesible para los potenciales interesados. Pero no sólo prestan esta importante función, sino que ofrecen al público un elenco de posibilidades creciente. Dentro de estas últimas, ocupa una posición de preeminencia, por el elevado uso que el público realiza del mismo, el servicio gratuito de correo electrónico.

[40] Sobre los eventuales problemas que está practica puede suponer frente a la propiedad intelectual, puede verse, entre otros, PEYRON, L. (1998) "I metatags di Internet como mezzo di contraffazione del marchio e di publicitá nasconta: un caso statunitense", *Giur. It.*, pp. 739-755; GARCÍA VIDAL, A. (2002) *Derecho de marcas e Internet*, Tirant lo Blanch, Valencia; ROSSI, J. D. (2002) "Protection for trademarks owners: The ultimate system of regulating search engine results", *Santa Clara L. Review*, Vol. 42, núm. 295, pp. 347-354; GARCÍA VIDAL, A. (2004) "La problemática de los enlaces en Internet". En MORO ALMARAZ, M. J. (Dir.) y APARICIO VAQUERO, J. P. y BATUECAS CALETRÍO, A. (Coords.), *Autores, consumidores y comercio electrónico*, Colex y Caja Duero, Madrid, pp. 347-378; SAMPOL PUCURRULL, M. (2005) "Administración Electrónica". En DE FUENTES BARDAJÍ, J. (Dir.) y PEREÑA PINEDO, I. (Coord.), *Manual de Derecho Administrativo Sancionador*, Thomson Aranzadi y Ministerio de Justicia, Navarra, pp. 1753-1776; ORTEGA DÍAZ, J. F. (2006) *Los enlaces en Internet. Propiedad intelectual e industrial y responsabilidad de los prestadores*, Thomson Aranzadi, Navarra; BUSTO LAGO, M. (2007) "La responsabilidad civil de los prestadores de servicios de la sociedad de la información". En REGLERO CAMPOS, L. F. (Coord.), *Tratado de responsabilidad civil*, Thomson Aranzadi, Navarra, pp. 2016-2118; LÓPEZ JIMÉNEZ, D. (2008) "Prácticas publicitarias electrónicas eventualmente vulneradoras de los derechos de propiedad intelectual e industrial", *La Notaría*, núm. 59-60, pp. 73-97; OTT, S. (2008) "Die Entwicklung des Suchmaschinen - und Hyperlink-Rechts im Jahr 2007", *WRP*, pp. 393-413; OTT, S. (2009) "Die Entwicklung des Suchmaschinen- und Hyperlink-Rechts im Jahr 2008", *WRP*, pp. 351-372.

Los buscadores requieren a sus usuarios registrarse para disfrutar, además de servicios de búsqueda, de otros como el de correo electrónico, páginas personales, el historial de búsquedas y otras prestaciones complementarias de la denominada *Web* 2.0 (por ejemplo, los *blogs*). De este modo, podría haber un registro de las actividades que el usuario lleva a cabo en la Red, permitiendo hacer perfiles de éste y utilizarlos por la empresa, pudiendo suceder que el usuario no fuera consciente ni estuviera suficientemente informado de esta circunstancia.

Entre los servicios personalizados destaca el servicio de correo electrónico. Los sistemas de correo electrónico que utilizan páginas *Web* como interfaz se conocen como "correo *Web*" -por ejemplo, *Yahoo Mail*, *Hotmail*, *Gmail*, etc.-. Se puede acceder al correo *Web* desde cualquier lugar y el usuario no necesita conectarse a un determinado proveedor de servicios de Internet, como cuando utiliza una cuenta normal de correo electrónico. Este suele ser gratuito, pero para obtener su cuenta los usuarios tienen que comunicar al proveedor datos personales –como el nombre y apellidos, fecha de nacimiento, lugar de residencia, etc.-.

Esta característica permite al proveedor de servicios de correo incorporar anuncios personalizados en la página HTML en la que éste se presenta -gráficamente, fuera del propio mensaje-. El correo *Web* depende, en gran medida, de patrocinadores por lo que es habitual que ofrezca publicidad. Tal extremo podría entenderse como una manifestación del conocido pacto "contenidos gratuitos a cambio de publicidad". No debe olvidarse, que como determina cierto sector de la doctrina[41], un elevado número de consumidores están dispuestos a aceptar publicidad o ceder datos y privacidad a cambio de recibir gratuitamente servicios sin tener que pagar por ellos.

Además, dado que los sistemas de correo *Web* se basan en el protocolo HTTP, pueden ser vulnerables a los mencionados *Web bugs*, pudiendo descubrir la identidad de correo electrónico de una persona mediante *cookies* y etiquetas HTML incrustadas[42].

Otro de los problemas que plantea el correo electrónico es el escaneo de los contenidos del mismo. Normalmente, esta filtración se realiza con el fin de prevenir virus –tanto para los usuarios como para los sistemas del responsable de

[41] GÓMEZ CASTALLO, J. D. (2010) "La privacidad ante las nuevas técnicas publicitarias. La apuesta de la autorregulación", *Telos: Cuadernos de Comunicación e Innovación*, núm. 82, pp. 11-17.

[42] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2007) "Declaración sobre buscadores de Internet", AEPD, Madrid.

tratamiento de datos (proveedor de servicios de correo electrónico)-, correo no deseado o *spam* –práctica también denominada buzonfia-, detectar contenidos potencialmente ilegales, corrección ortográfica, el reenvío de mensajes, la auto-respuesta, la señalización con banderas de mensajes urgentes, la conversión de correos electrónicos entrantes en mensajes de texto de móvil, el salvado automático, pero, lo que es verdaderamente relevante a nuestros efectos, para remitir publicidad personalizada según el contenido del mensaje –recibido y/o enviado-. De esta manera, se podrán ofrecer, bajo la modalidad de anuncios patrocinados, mensajes comerciales, según los términos incluidos en el mensaje, sobre bienes y/o servicios relacionados. Esta última práctica puede transgredir la confidencialidad de las comunicaciones por correo electrónico reconocida por la normativa internacional[43], comunitaria[44] y nacional[45].

[43] La confidencialidad de las comunicaciones está garantizada según los instrumentos internacionales relativos a los derechos humanos, sobre todo, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950. El art. 8 de este último establece que toda persona tiene el derecho al respeto de su vida privada y su correspondencia, y define las condiciones en las que podría aceptarse la restricción de estos derechos.

[44] Debemos, al menos, citar cuatro Directivas al respecto así como una Propuesta de Directiva. Por lo que a las primeras se refiere, la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuyo art. 16 versa sobre la confidencialidad del tratamiento y el art. 17 sobre la seguridad de este último; la Directiva 2002/58/CE del relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas –fundamentalmente los arts. 4 relativo a la seguridad de las comunicaciones y 5 sobre confidencialidad de las mismas-; y la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, cuyo art. 15 incluye ciertas disposiciones relativas a la responsabilidad de los proveedores de servicios Internet o correo electrónico con arreglo a las cuales los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisión. Esta obligación constituiría una violación de la libertad de información así como de la confidencialidad de la correspondencia; y la Directiva 2006/24/ sobre conservación de datos de tráfico generados en las comunicaciones electrónicas, que no sólo modifica la Directiva 2002/58/CE, sino que, además, introduce importantes y discutidas novedades a propósito del tratamiento de datos personales del tráfico y localización generados por el uso de los servicios de comunicaciones electrónicas. En cuanto a la Propuesta de Directiva, a la que antes aludíamos, cabe decir que se trata de la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, de 13 de noviembre de 2007, que añade una garantía relevante para los usuarios, dado que "en caso de violación de la seguridad que

El Grupo de Trabajo del Artículo 29, se ha pronunciado sobre este asunto en el Dictamen 2/2006, de 21 de febrero de 2006, analizando los supuestos en los que los buscadores pueden escanear el contenido de los correos electrónicos, estableciendo que únicamente se podrán filtrar las comunicaciones con la finalidad de prevenir virus y *spam*, para adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, según dispone el artículo 4 de la Directiva 2002/58/CE de privacidad en las telecomunicaciones, que se transpone en el artículo 34 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

En cuanto al análisis de contenidos, a efectos de impedir la entrada de virus en los sistemas tanto propios como del usuario –que, en la inmensa mayoría de los casos, es automático siendo parte del servicio-, cabe decir que tal acto se justificaría para preservar la seguridad de los servicios, de conformidad con el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas y por ser necesario para la mera ejecución del contrato de servicio suscrito con sus clientes, que esperan recibir y enviar correos con un cierto grado de seguridad, de conformidad con el artículo 7.b) de la Directiva de protección de datos, sin perjuicio de la confidencialidad de la comunicación.

Respecto al análisis de correos electrónicos para evitar el *spam* –que puede definirse como toda aquella comunicación publicitaria no solicitada (que, normalmente, tiene como fin ofertar, comercializar o tratar de despertar el interés de un determinado producto, servicio y/o empresa) que llegue tanto al buzón de correo electrónico[46] -, que, además, vulnera la privacidad de sus destinatarios[47] ,

provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la difusión o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de servicios de comunicaciones disponibles al público en la Comunidad, el proveedor de los servicios de comunicaciones electrónicas disponibles al público notificará dicha violación al abonado afectado y a la autoridad nacional de reglamentación sin dilaciones indebidas".

[45] En este sentido, Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal y su Reglamento de desarrollo; la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones; y la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[46] BURGOS y LUZ DE LEÓN, D. (2001) *Comercio electrónico, publicidad y marketing en Internet*, McGraw-Hill, Madrid; MIQUEL RODRÍGUEZ, J. (2001) "Problemática jurídica de la publicidad en Internet". En BOTANA GARCÍA, G. A. (Coord.), *Comercio Electrónico y Protección de los Consumidores*, La Ley, Madrid, pp. 245-274; TATO PLAZA, A. (2004) "La publicidad en Internet". En GONZÁLEZ DELGADO, J. A. (Coord.), *Responsa iurisperitorum digesta*, Vol. 5, Ediciones de la

ha de señalarse que es una práctica necesaria dado que de omitirse los sistemas serían probablemente muy lentos e ineficaces, malográndose, de este modo, la utilidad del correo electrónico para sus usuarios. Esta situación no satisfaría a los consumidores, reduciendo las posibilidades de proporcionar un servicio de correo electrónico fiable y digno de confianza. Tal operación de análisis estaría legitimado por el artículo 7.b) de la Directiva de protección de datos, ya que el filtrado para combatir el *spam* es necesario para que el proveedor de correo electrónico pueda ejecutar correctamente el contrato del que es parte el afectado por los datos, es decir, el destinatario del mensaje.

Aún así, los proveedores de servicios deben informar sobre sus prácticas de cribado de correo electrónico y ofrecer a sus abonados la posibilidad de decidir sobre el filtrado para evitar el *spam*. Fuera de estos casos, en los que los correos se escanean por motivos de seguridad del servicio, la interceptación de contenidos con fines publicitarios no resultaría conforme a la legislación española en materia de protección de datos y de contratación electrónica.

En este último sentido, podría estar incluso vulnerándose el art. 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico que prohíbe la remisión de comunicaciones comerciales no solicitadas que preceptúa que "1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas; 2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales

Universidad de Salamanca, Salamanca, pp. 89-104; TATO PLAZA, A. (2004) "La publicidad en Internet". En MORO ALMARAZ, M. J. (Dir.) y APARICIO VAQUERO, J. P. y BATUECAS CALETRÍO, A. (Coords.), *Autores, consumidores y comercio electrónico*, Colex y Caja Duero, Madrid, pp. 141-156; GUILLÉN CATALÁN, R. (2005) *Spam y comunicaciones comerciales no solicitadas*, Thomson Aranzadi, Navarra.

[47] RUIZ MIGUEL, C. (2001) "Protección de datos personales y comercio electrónico". En GÓMEZ SEGADE, J.A. (Dir.), *Comercio electrónico en Internet*, Marcial Pons, Madrid, pp. 408 y 409; TATO PLAZA, A. (2001) "Aspectos jurídicos de la publicidad y de las comunicaciones comerciales en Internet". En GÓMEZ SEGADE, J.A. (Dir.), *Comercio electrónico en Internet*, Marcial Pons, Madrid, pp. 222-223; VEGA VEGA, J. A. (2006) "La publicidad comercial...", cit., pp. 92 y 93; VEGA VEGA, J. A. (2009) "Contratación electrónica, mercado y derecho", *Revista de Estudios Económicos y Empresariales*, núm. 21, pp. 108-109 y 118-120.

referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija". A tenor de lo establecido en el art. 21.2 LSSI-CE[48], podemos determinar que la remisión de comunicaciones comerciales, en tal supuesto, será lícita siempre que concurran, con carácter necesario, los siguientes presupuestos[49]: 1. Que exista una relación contractual previa que no es necesario que subsista en el momento de operarse la comunicación. La disposición que comentamos alude a una relación contractual perfeccionada y ejecutada y no al simple contacto propio de la fase precontractual[50] –donde deberán entenderse incluidas las intenciones de contratar, contratos previos no conclusivos o, qué duda cabe, tratos preliminares-; 2. Los datos de contacto con el destinatario deben haberse obtenido de forma lícita, lo que presupone, como regla general, el cumplimiento de los deberes de información al titular de los datos y de recabar el consentimiento del mismo para su tratamiento, salvo en los supuestos expresamente previstos en la legislación de protección de datos y; 3. Dichos datos únicamente pueden establecerse para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

---

[48] Sobre los problemas de interpretación que tal norma suscita, en la práctica, puede verse PANIZA FULLANA, A. (2004) "Comunicaciones comerciales no solicitadas y marketing directo: el sistema *opt out* como excepción (correo electrónico y mensajes SMS con fines publicitarios)". En RAMOS, B. y RIBAGORDA, A. (Dirs.), *Avances en criptografía y seguridad de la información*, Díaz de Santos, Madrid, pp. 437-445.

[49] DE ASÍS ROIG, A. E. (2004) "Comentarios a la Disposición Final Primera". En GARCÍA DE ENTERRÍA, E. y DE LA CUADRA-SALCEDO, T. (Coords.), *Comentarios a la Ley General de Telecomunicaciones, Ley 32/2003, de 3 de noviembre*, Thomson Aranzadi, Navarra, pp. 1205-1218.

[50] RODRÍGUEZ DE LAS HERAS BALLEL, T. (2006) "La formación del contrato en el entorno electrónico y los procedimientos electrónicos de contratación". En CALVO CARAVACA, A. L. y CARRASCOSA GONZÁLEZ, J. (Dirs.), *Estudios sobre Contratación Internacional*, Colex, Madrid, pp. 535-572. En sentido contrario, 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, p. 117, quien considera que deben entenderse incluidas las negociaciones preliminares.

Existen dos máximas que, en relación con la remisión de comunicaciones comerciales, siguen vigentes, de acuerdo con la LSSI-CE, incluso después de su modificación[51]. Por un lado, dichas comunicaciones realizadas por vía electrónica, se rigen por lo dispuesto en la Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal[52] (en adelante LOPD), en lo que respecta a la obtención de datos, información a los interesados, y creación y mantenimiento de ficheros –art. 19 LSSI-CE-, y, por otro lado, las referidas comunicaciones comerciales deben ser claramente identificables, indicando la persona física y jurídica en nombre da la cual se realizan[53], e incluyendo la palabra "publicidad" o la abreviatura "publi", en virtud de la modificación operada por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, cuando se haga a través de correo electrónico u otro medio de comunicación electrónica –art. 20 LSSI-CE-.

En línea con las apreciaciones formuladas, existen supuestos que podrían entrar en contradicción con la normativa legal, cual es el caso del correo electrónico de *Google*, más conocido como *Gmail*. Se trata de un servicio que ofrece ciertas ventajas con respecto a sus competidores, dado que, a diferencia de estos últimos,

[51] PIÑAR MAÑAS, J. L. (2004) "La protección de datos en las comunicaciones comerciales en Internet y los nuevos medios", *Revista Autocontrol de la Publicidad*, núm. 85.

[52] Ciertos autores, como GRIMALT SERVERA, P. (2005) "Deberes y responsabilidades en materia de protección de datos". En CAVANILLAS MÚGICA, S. (Coord.), *Deberes y responsabilidades de los servicios de acceso y alojamiento. Un análisis multidisciplinar*, Comares, Granada, pp. 183-201, aluden a la eventual interferencia que podría plantearse entre la LOPD y la LSSI-CE, por lo que podríamos preguntarnos si nuestro ordenamiento jurídico prohíbe el envío de publicidad a través del correo electrónico –u otros medios de comunicación electrónica equivalentes-, salvo que el correo electrónico se haya obtenido de una fuente accesible al público –es decir, en este caso, lo establecido en la LOPD excepcionaría a la LSSI-CE- o si, por el contrario, hay que entender que si los datos se han obtenido de fuentes accesibles al público pueden ser empleados para fines promocionales, salvo que se trate de comunicaciones por correo electrónico u otro medio equivalente, es decir, sería la LSSI-CE la que excepcionaría a la LOPD.

[53] Debemos aclarar que, en numerosas ocasiones, las empresas que realicen el envío efectivo de las comunicaciones comerciales electrónicas serán entidades contratadas por las agencias de publicidad. En consecuencia, la empresa que remite las comunicaciones comerciales electrónicas no siempre coincidirá con la que promociona el bien y/o servicio. En atención a tales considerandos, 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, pp. 120 y 121, entiende que hubiera resultado más oportuno que el legislador hubiera establecido la necesidad de incluir en el mensaje los datos del remitente efectivo del mensaje.

presenta una capacidad de almacenamiento sensiblemente mayor, ofrece la posibilidad de buscar en los mensajes a través de palabras clave, realiza la organización de los mensajes por hilos de conversación que permite que los usuarios visualicen los correos electrónicos iniciales y sus respectivas respuestas como una cadena de toda la conversación y no como mensajes individuales, etc. En todo caso, es necesario señalar que Gmail recurre a *Adsense* de *Google*[54] para incluir publicidad contextual junto a los mensajes de correo electrónico, lo que supone que un *bot* –un determinado tipo de programa informático- lee el contenido de los correos. Aunque los responsables de *Gmail* disponen que ningún humano tiene acceso a las comunicaciones, lo cierto que, insistimos, tal práctica con fines publicitarios podría estar vulnerando, por lado, la privacidad de los titulares de tales cuentas de correo electrónico y de los usuarios que, a su vez, les remitan correos (que tampoco escapan al escaneo con tales fines) y, por otro, la prohibición de remitir comunicaciones comerciales no solicitadas, a las que, dicho sea de paso, ya hemos hecho alusión.

4. LA GEOLOCALIZACIÓN EN EL ÁMBITO DE LAS REDES SOCIALES Y SU REPERCUSIÓN EN MATERIA COMERCIAL

Una novedosa técnica publicitaria respecto a los medios móviles es la denominada geolocalización o georeferenciación[55] -o, en el lenguaje anglosajón, *location based services*- a la que, pese a su limitado uso actual, se augura –en el

[54] El servicio *adwords adsense* es una prestación publicitaria ofrecida por el buscador *Google* en virtud de la cual se concede a la empresa que lo contrata el derecho a anunciarse, bien como enlaces o resultados patrocinados, junto a los resultados de la búsqueda en Internet de una determinada palabra bien en el caso de que la palabra sea incluida en un mensaje remitido o recibido a través de Gmail. Debemos, al menos, señalar, como prestación significativa, el dato de que cuando se le hace una sugerencia al buscador *Google*, éste no sólo presenta palabras en plural o asociadas a lugares o adjetivos sino también sinónimos u otras variaciones contextuales de la misma palabra como recomendación.

[55] Para más información, puede verse WELLHOFF, A. y MASSON, J.E. (2000) *Rentabilidad y gestión en el punto de venta. El merchandising*, Ediciones Deusto, Bilbao, p. 242; CHASCO IRIGOYEN, C. (2003) "El Geomarketing y la Distribución Comercial", *Investigación y Marketing*, núm. 79, pp. 6-14; LONGLEY, P.A. y MATEOS RODRÍGUEZ, P. (2005) "Un nuevo y prominente papel de los SIG y el Geomarketing en la provisión de servicios públicos", *GeoFocus*, núm. 5, pp. 1-5; XU, H. TEO, H. H. y TAN, B.C.Y. (2005) "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk", *Proceedings of 26th Annual International Conference on Information Systems*

medio plazo- una enorme proyección y potencial de crecimiento[56]. Constituye un servicio cuya funcionalidad básica estriba en localizar la ubicación espacio-temporal de un determinado dispositivo móvil[57]. De esta manera, es posible, cuando se efectúa el acceso a algún sitio *Web*, captar información sobre los movimientos del usuario, así como sus requerimientos, con el fin de rediseñar la oferta comercial.

Se trata de políticas de marketing que, basándose en la localización geográfica, permiten, por ejemplo, bloquear el acceso del navegante, en función de su origen geográfico, a un sitio de la Red, redireccionarlo a alguna sección o enlace electrónico determinado. Algunas de estas últimas funciones son posibles en virtud del navegador *Mozilla Firefox*, o del navegador de Google –*Chrome*-. También, recientemente, la geolocalización se sirve de la realidad aumentada. Esta última se basa en la superposición de información virtual sobre un determinado objeto o imagen de forma digital. Esta es, precisamente, la principal diferencia con la realidad virtual, ya que no sustituye la realidad física, sino que sobreimprime los datos informáticos al mundo real, haciendo, en nuestro caso, que la información geolocalizada sea más natural.

Este aspecto, *a priori*, supone ventajas tanto para el propio usuario como para las empresas a las que las comunicaciones comerciales aludirán. Por lo que a los usuarios se refiere, podrán recibir mensajes personalizados sobre bienes y/o servicios, cercanos al lugar en el que en cada momento se encuentren, que puedan ser de su interés. Respecto a las empresas que empleen esta técnica, cabe decir

(ICIS), Las Vegas, Nevada, pp. 897-910; XU, H. (2007) "Privacy Considerations in the Adoption of Location-Based Services: A Psychological Control Perspective", *Proceedings of 67th Annual Meeting of the Academy of Management* (AOM), Philadelphia, PA; XU, H. y GUPTA, S. (2009) "The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers' Adoption of Location-Based Services", *Electronic Markets - The International Journal on Networked Business*, Vol. 19, núm. 2, pp. 137-149; XU, H. TEO, H. H. TAN, B.C.Y. y AGARWAL, R. (2009) "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services", *Journal of Management Information Systems*, Vol. 26, núm. 3, pp. 137-176.

[56] Tales consideraciones se extraen del estudio realizado en 2010 por *Forrester Research* del que se deduce que, en la actualidad, únicamente el 4% de los usuarios adultos de Estados Unidos ha usado, al menos una vez, algún servicio de geolocalización, si bien en el medio plazo su empleo será creciente.

[57] Sobre este particular, se recomienda la lectura de la Comunicación de la Comisión francesa de protección de datos -*Commission nationale de l'informatique et des libertés*-, de 5 de febrero de 2009, sobre la publicidad en línea dirigida a grupos específicos, disponible en el siguiente enlace electrónico: http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD.pdf, pp. 19-20.

que existe la posibilidad de que la promoción, dada la elevada personalización y segmentación, obtenga una importante eficacia[58]. Se trata, en definitiva, de asociar lugares –así, por ejemplo, museos, restaurantes, parques, oficinas, cines, o cualquier otro lugar del mundo del ocio y/o la cultura- del mundo real con la situación espacio-temporal de los usuarios utilizando, como plataforma que virtualmente conecte ambos agentes, la red social.

En todo caso, además de las ventajas mencionadas, existen inconvenientes vinculados, en gran medida, a la posible violación de la privacidad de los usuarios de los dispositivos móviles[59]. En efecto, si el simple uso de Internet implica riesgos, a efectos de privacidad, la puesta en práctica de algunas técnicas publicitarias, como las que analizamos -geolocalización-, van más allá, dado que permiten identificar al usuario, individualizarlo e, incluso, hacerle un seguimiento personal[60]. En este sentido, en opinión de ciertos autores[61], en los dispositivos móviles pueden instalarse mecanismos electrónicos susceptibles de monitorizar el comportamiento –como las *cookies*- lo que, unido a la geolocalización del usuario, permitiría su identificación completa. Aunque fue un servicio ofrecido originariamente por varios sitios *Web* –como *Foursquare*, *Gowalla*, *Brightkite* y *Loopt*- lo cierto es que inicialmente su uso no se consolidó, tendencia que parece haber cambiado con las redes sociales, dado que representa una prestación muy aceptada por parte del público usuario de las mismas. En este sentido, algunas de ellas, como *Twitter*, *Foursquare* y *Facebook*, ya recurren a esta novedosa técnica publicitaria, mientras que otras se plantean hacerlo en el futuro inmediato.

Dado que los datos expuestos en los perfiles de las redes sociales pueden comportar, en numerosas ocasiones, problemas de privacidad para sus titulares, de manera acertada, los criterios de configuración de las mismas optan por conceder al servicio de geolocalización un elevado nivel de protección de la

[58] En este sentido, GASIMOV, A. TAN, C. H. PHANG, C. W. y SUTANTO, J. (2010) "Visiting Mobile Application Development: What, How and Where", *Proceedings of the 9th International Conference on Mobile Business* (ICMB), Atenas (Grecia).

[59] Sobre este particular, sugerimos VON BREDOW, R. DWORSCHAK, M. MÜLLER, M. U. y ROSENBACH, M. (2010) "Ende der Privatheit", *Der Spiegel*, núm. 2, http://www.spiegel.de/spiegel/print/d-68621901.html.

[60] VÁZQUEZ RUANO, T. (2008) *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Marcial Pons, Madrid-Barcelona, pp. 262 y 263.

[61] MESSÍA DE LA CERDA BALLESTEROS, J.A. (2004) *La protección de datos de carácter personal en las telecomunicaciones*, Dykinson, Madrid, p. 136.

privacidad. Es lo que, con carácter general, se ha denominado por parte del Supervisor Europeo de Protección de Datos, intimidad mediante el diseño[62]. De esta manera, suele estar desactivado, por defecto, por lo que para activarlo deberá operarse voluntariamente su puesta en práctica.

En todo caso, si el proceder de las redes sociales no fuera, en todos los supuestos, el planteado, podrían suscitarse ciertos problemas. En efecto, a título de ejemplo, cuando el titular del perfil realizase la indicación de su posición en un determinado instante podría ser visible no solo por sus contactos sino por cualquier usuario –registrado o, en su caso, no registrado- de la red social. Otro caso espinoso podría ocasionarse cuando un contacto admitido de un usuario de la red social (denominado, de manera coloquial, "amigo") etiquetara –sin su consentimiento expreso- a este último en un lugar en un preciso instante. Tal acto, que podría resultar eventualmente pernicioso para el afectado, debería requerir del consentimiento de este último para que no se vulnerase su privacidad. En otros términos, para que un usuario admitido por otro u otros pudiera fijar la posición espacio-temporal de uno o varios de sus contactos, debería ser preceptivo contar con el consentimiento previo de los mismos. Naturalmente, dado que teóricamente también cabría la posibilidad de etiquetar a efectos de localización, a personas todavía no integradas en la red social, lo más aconsejable sería, para salvaguardar la privacidad de estas últimas, no permitir tal extremo. En última instancia, como hemos planteado anteriormente, lo más racional sería establecer, por defecto, el nivel más alto posible de protección de la privacidad. De este modo, serían posteriormente los propios usuarios los que, en atención a sus necesidades o deseos, podrían, de manera consciente, habilitar progresivamente más opciones.

A tenor del art. 3 de la Directiva 2002/58/CE, la misma resulta aplicable al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad. En aplicación de lo dispuesto en el art. 4 de la Directiva 95/46/CE, la legislación nacional aplicable es la del Estado miembro en que esté establecido el responsable del tratamiento. Esta disposición supone

[62] Sobre este extremo, recomendamos la consulta del Dictamen del Supervisor Europeo de Protección de Datos, de 18 de marzo de 2010, relativo a "La Promoción de la confianza en la sociedad de la información mediante el fomento de la protección de datos y la privacidad", disponible electrónicamente en http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

que, dentro de la Comunidad, el tratamiento de los datos de localización está sujeto a la normativa nacional del Estado miembro en el que esté establecido el responsable del tratamiento y no a la del Estado miembro del que sea nacional el interesado. En el supuesto de que el responsable del tratamiento -el proveedor del servicio con valor añadido- no esté establecido en un Estado miembro, los datos de localización únicamente podrán transferirse del operador de comunicaciones electrónicas al responsable del tratamiento en las condiciones establecidas en el capítulo IV de la Directiva 95/46/CE relativo a la transferencia de datos personales a países terceros.

Para evitar que tales prácticas electrónicas vulneren, de forma flagrante, la normativa imperante en materia de protección de datos de carácter personal[63] es preceptivo que el afectado otorgue su consentimiento y sea informado de las condiciones de dicho tratamiento –art. 9 Directiva 2002/58-[64]. Tal declaración de voluntad deberá realizarse de manera libre, específica, informada e inequívoca[65]. La forma de operar tal manifestación podrá ser diversa. Así, por

[63] Existen numerosos supuestos en los que, en la práctica, se ha vulnerado la normativa imperante en materia de privacidad como consecuencia de la remisión de comunicaciones comerciales electrónicas a teléfonos móviles sin contar con el consentimiento de sus titulares. Así lo ha entendido la Agencia Española de Protección de Datos en diversos procedimientos sancionadores (PS): PS 0006/2005 y PS 00027/2005, entre otros.

[64] MEDINA MALO DE MOLINA, E. (2003) "Comunicaciones comerciales por vía electrónica: códigos de conducta, resolución judicial y extrajudicial de conflictos". En MATEU DE ROS CEREZO, R. y LÓPEZ-MONIS GALLEGO, M. (Coords.), *Derecho de Internet: la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Thomson Aranzadi, Navarra, p. 522.

[65] Sobre este aspecto, entre otros muchos, GRIMALT SERVERA, P. (2005) "Deberes y responsabilidades en materia de protección de datos". En CAVANILLAS MÚGICA, S. (Coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Comares, Granada, pp. 165-202; PIÑAR MAÑAS, J.L. (2005) "Derecho fundamental a la protección de datos", *Asamblea: revista parlamentaria de la Asamblea de Madrid*, núm. 13, pp. 21-46; DEL VALLE MECED, M. (2006) "El tratamiento de datos de carácter personal (comentario a la sentencia de la Audiencia Nacional de 18 de enero de 2006)", *La Ley*, núm. 3, pp. 1824-1829; CANALES GIL, A. (2007) "El derecho fundamental a la protección de datos de carácter personal", *Revista Jurídica de Castilla y León*, núm. 12, pp. 13-56; GRIMALT SERVERA, P. y CAVANILLAS MÚGICA, S. (2008) "Servicios de la sociedad de la información y protección de datos personales". En *Derecho de la Empresa y Protección de Datos*, Thomson Aranzadi y Agencia Española de Protección de Datos, Navarra, pp. 329-336; LESMES SERRANO, C. (2008) *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Tirant lo Blanch, Valencia, pp. 118 y 189-199; PUENTE ESCOBAR, A. (2008) "Consentimiento del afectado y deber de información". En MARTÍNEZ MARTÍNEZ, R. (Coord.), *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*, Tirant lo Blanch, Valencia, pp. 37-62.

ejemplo, podrá lograrse a través de la aceptación de las cláusulas generales de la contratación del uso del terminal móvil o de la red inalámbrica en base a la cual acceda a Internet, o de la configuración del dispositivo móvil para ser localizado y, en consecuencia, recibir publicidad personalizada, o cada vez que se haga uso del servicio en cuestión. En el caso de que el consentimiento se haya dado mediante la aceptación de cláusulas generales, los interesados deben tener la oportunidad de consultar, de nuevo, la información cuando lo deseen y, además, de forma simplificada como, por ejemplo, podría ser la habilitación de un determinado apartado, al efecto, en un sitio *Web*[66].

De acuerdo con la Directiva 2002/58/CE –Considerando 35-, en los casos en que los usuarios hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización[67]. El reconocimiento permanente del derecho a oponerse al tratamiento de los datos de localización es esencial teniendo en cuenta el carácter especialmente sensible de los mismos.

Como vimos, a propósito del análisis de la publicidad basada en la navegación del usuario, se han elaborado iniciativas, fruto del fenómeno de la autorregulación de la industria para, precisamente, complementar –preferentemente en beneficio de la privacidad del consumidor y/o usuario- las normas elaboradas por el legislador. Tales prácticas también concurren en el caso del geomarketing. Entre las mismas, cabe hacer alusión al manual de buenas prácticas para las aplicaciones basadas en la localización, elaborado por *CTIA-The Wireless Association*, cuya última versión data de marzo de 2010[68] –siendo su primer borrador de 2008-. El documento de buenas prácticas mencionado incide en, al menos, dos cuestiones destacables. Por un lado, alude a la necesidad de avisar al potencial usuario del servicio, sobre cómo se utilizará la información de su localización, será implementada y protegida para que los titulares puedan tomar decisiones sobre

[66] Así lo determina, de manera expresa, el Grupo de Trabajo del Artículo 29 en el Dictamen 5/2005, de 25 de noviembre de 2005, sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido.

[67] Sobre este particular, en la legislación española, el art. 70 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

[68] El texto, en su versión completa, puede verse en el siguiente enlace electrónico: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.

si utilizar o no el servicio, o, en su caso, optar por la plena privacidad de sus datos. Y, por otro, deberá recabarse el consentimiento expreso del mismo, dado que, una vez que los usuarios hayan permitido servicios basados en la localización, o, incluso, fijado un nivel alto de privacidad sobre la información de su emplazamiento, deberían tener la posibilidad de determinar si la localización puede ser protegida frente a terceros así como la manera de revocar dicha autorización.

5. CONCLUSIONES

La protección de los datos de carácter personal es una cuestión extraordinariamente importante en el espacio comunitario. Tal aspecto ha suscitado, en ocasiones, ciertos problemas con empresas establecidas en los Estados Unidos –como *Google* o *Facebook*- que tratan datos personales de usuarios de la Unión Europea.

Lejos de hacer de la privacidad un aspecto baladí, los nuevos modelos que permiten socializar la Red y, en concreto, las prácticas vinculadas con la publicidad comportamental, están adaptándose a las directrices establecidas por las normas europeas y nacionales sobre el particular. En efecto, las empresas son cada vez más conscientes de las consecuencias que puede representar para las mismas una deficiente política de privacidad, que no es sino aquella que no considera las implicaciones de las acciones comerciales y los nuevos productos en la privacidad.

Hasta hace relativamente poco tiempo, las acciones publicitarias desarrolladas en Internet se desarrollaban, en gran medida, fundamentadas sobre la identificación anónima del usuario, lo que determinó la relativa aceptación de las mismas y, con ello, una cierta confianza. Ahora bien, recientemente, se han puesto en práctica técnicas comerciales cada vez más agresivas que pueden comprometer la privacidad de los usuarios. En este sentido, nos hemos referido a diferentes tácticas que, directa o indirectamente, podrían englobarse en el ámbito de la publicidad comportamental, como las *cookies*, los *spyware*, troyanos *web bugs* y otros instrumentos técnicos, que se fundamentan en la navegación realizada por el usuario, y algunas actuaciones realizadas en el marco de los correos electrónicos gratuitos, como el paradigmático caso de Gmail, en el que las palabras presentes en los correos enviados y/o recibidos por su titular, determinan la puesta en práctica de ciertos anuncios en la parte superior de la interfaz de Gmail. No

puede, en modo alguno, dejarse de lado novedosas técnicas, a las que en cada vez más casos se recurren por las redes sociales, como es la geolocalización.

Aunque todas ellas parecen haber sido concebidas para desplegar una elevada eficacia en el campo de la publicidad comportamental, lo cierto es que, como sistemáticamente hemos puesto de manifiesto, pueden vulnerar la privacidad. Con buen criterio, las autoridades comunitarias han aprobado un elenco nada desdeñable de normas, posteriormente incorporadas a los ordenamientos internos de los diferentes Estados, para garantizar la protección de los datos de carácter personal. En todo caso, lo ideal resulta, como el propio legislador preceptúa, que tal legislación sea complementada en virtud del fenómeno de la autorregulación de la propia industria. Una de las ventajas apreciables de este último reside en que los documentos en que se materializan –habitualmente códigos de conducta- no restringen su eficacia al territorio de un determinado Estado, dado que muchos de ellos presentan una marcada vocación transnacional. No debe olvidarse su rápida y constante adaptación a los cambios acontecidos en los aspectos reglamentados –lo que parece especialmente importante en la materia que abordamos-.