# MARKETING COMPORTAMENTAL EN LINEA

## El desafío de las cookies

María José Viega Rodríguez

# MARKETING COMPORTAMENTAL EN LINEA

## El desafío de las cookies

**Dra. María José Viega Rodríguez**

**Montevideo, Julio de 2012**

# PROLOGO

El libro de la Dra. María José Viega que me honro en prologar trata un tema de plena actualidad y relevancia, que se relaciona con la sociedad de la información y del conocimiento y, por cierto, con las situaciones jurídicas de diversos actores de la misma.

Efectúa un análisis interdisciplinario y tiene un explícito enfoque garantista en materia de datos personales, con adecuado énfasis en el previo consentimiento informado del titular de esos datos, específicamente como cliente.

La obra se estructura en cinco Capítulos, *respectivamente "Introducción al Marketing electrónico"; "Protección de Datos: amenazas y publicidad"; "Marco Normativo"; "Marketing Comportamental en Línea*" y "*Situación Actual".* Aparecen precedidos por líneas tituladas "*A modo de presentación*", en las que se sitúa adecuadamente el objeto en estudio –aspecto específico de la publicidad efectuada por medios electrónicos – y la incidencia que estos tienen al permitir la trazabilidad del perfil del potencial cliente.

Con una exposición técnicamente fundada y un desarrollo claro, práctico y ameno, la autora considera, entre otras cuestiones, la forma de actuación de espías en Internet –sean gobierno, empresas o ciberdelincuentes – con ejemplos de sus aplicaciones; la evolución permanente que se verifica en los medios técnicos, caso de una nueva generación o de derivados del phising; los servicios que pueden prestar las cookies y los desafíos que presentan, etc.
Al tratar el Marco Normativo, específicamente los de la Unión Europea, España, Argentina y Uruguay, examina su régimen de derecho positivo, en su caso con ajustes recientes, como el Real Decreto español 13/012, y de situaciones planteadas en dichos sistemas. Ello sin perjuicio de tener presente la autorregulación en el sector, tema que desarrolla en el Capítulo V; en este efectúa, además, una reseña del estado de situación sobre el uso de las cookies en el ámbito europeo.

En el Capítulo IV está lo que –en términos de la autora – es *"el corazón del trabajo"***.** Allí estudia el marketing conductual, noción que es traducción de "*on line behavorial advertising" (OBA),* cuya definición por parte de la Comisión Federal de Comercio de EEUU cita (seguimiento de la actividad de los consumidores en línea –búsquedas, páginas web visitas, contenido – para ofrecer publicidad). Entre otros aspectos, trata de la clasificación del marketing en línea –contextual, segmentado, comportamental; respecto de este último refiere a las técnicas de rastreo, entre ellas, precisamente las cookies instaladas en el navegador de los usuarios; los tipos de OBA; etc.

Destaca las funciones y responsabilidades de los actores involucrados – proveedores de redes de publicidad, editores y anunciantes – acorde con su actividad y modalidades de actuación; en el primer caso, subraya que la configuración del navegador no implica consentimiento.

En todo caso, a la vez que se tiene en cuenta la utilidad de la publicidad electrónica, se destaca la importancia de la seguridad y de la protección del usuario-consumidor, en especial a través del previo y debidamente informado consentimiento –eje del sistema – cuya pertinencia se estudia según las situaciones consideradas. Con razón se entiende que lo relevante no es descubrir nuevos principios y derechos, sino aplicar adecuadamente los vigentes en el correspondiente entorno socio-económico, político y tecnológico; también la conciencia personal, en cualquier entorno, de que “nosotros somos los primeros custodios de nuestros datos personales (…)”.

En suma, estamos ante una obra de interés académico y práctico sobre la publicidad y comunicación comercial desde una perspectiva amplia, tanto de la tecnología informática/ telemática como del derecho; con ella la Dra. Viega añade otro valioso aporte a una temática que la cuenta como cultora de excelencia.

Felipe Rotondo Tornaría

Profesor de Derecho Administrativo

Miembro de la Unidad Reguladora y de

Control de Datos Personales

## CURRICULUM DE LA AUTORA

María José Viega Rodríguez es:

Doctora en Derecho y Ciencias Sociales, Escribana Pública y Profesora Adscripta en Informática Jurídica por la Universidad Mayor de la República Oriental del Uruguay (UDELAR).

Directora del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad de la República.

Directora del Estudio Jurídico Viega & Asociados www.viegasociados.com

Gerente de Derechos Ciudadanos (Ciudadanía Digital) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) – Presidencia de la República.

Profesora de Derecho Informático y Derecho Telemático, Coordinadora del Grupo del Jurisprudencia del Instituto de Derecho Informático y Ex - Profesora del curso en línea Derecho del Ciberespacio en la UDELAR.

Realizó cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires.

Experta Universitaria en Protección de Datos (UNED – España)

Especialista en Administración Electrónica (UOC – España)

Ex - Profesora de Derecho de las Telecomunicaciones en la Universidad de la Empresa.

Ex - Profesora en la Oficina Nacional de Servicio Civil (Presidencia de la República) del Curso Derecho de Internet.

Ex - Profesora de los cursos de e-learning “Introducción al Derecho de las TICs”, “Documento y firma electrónica”, “Protección de datos” y “Contratos Informáticos” en Viega & Asociados.

Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico (APADIT)

Miembro Fundador del Instituto de Derecho Informático (UDELAR) y de FIADI Capítulo Uruguay.

Miembro de la International Technology Law Association y de la International Association of Privacy Professionals.

Autora de los libros:

- “Contratos sobre bienes y servicios informáticos”. Amalio Fernández, junio 2008.

Co-autora de los Libros:

- con el Dr. Carlos Delpiazzo: Lecciones de Derecho Telemático Tomo I y II (FCU, abril 2004 y mayo 2009)

- con la Dra. Esc. Beatriz Rodríguez del e-book “Documento Electrónico y Firma Digital. Cuestiones de Seguridad en las Nuevas Formas Documentales (junio 2005)

- con la Dra. Esc. Beatriz Rodríguez y Flavia Baladán de “Marco normativo del Derecho Informático” (julio 2011)

- con la Dra. Esc. Beatriz Rodríguez “Documento y Firma. Equivalentes funcionales en el mundo electrónico”. En proceso de edición, junio 2012.

Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

## A MODO DE PRESENTACION

Frente al avance de las tecnologías y la preocupación por parte de las autoridades de protección de datos en relación con la creación de perfiles con fines de publicidad y marketing, nos ha parecido éste un tema de interés y actualidad para investigar.

Sin lugar a dudas, tiene una trascendencia económica para las empresas publicitarias, para los sitios web que ofrecen diferentes servicios por sí y a éstas, por lo cual un correcto asesoramiento desde el punto de vista jurídico es vital, a la hora de cumplir la normativa y brindar un servicio respetuoso del derecho de los consumidores y sobre todo de la protección de los datos personales.

El tema tiene relevancia política, ya que el acceso a la tecnología, el conocimiento sobre la misma, nos abre un nuevo horizonte, y como todo conocimiento nos hace más libres en nuestras elecciones y nos permite observar los aconteceres mundiales desde una óptica diferente. El conocimiento de las diferentes herramientas utilizadas en el ciberespacio para captar nuestra información nos permite autodeterminarnos informativamente, y sopesar los beneficios, pero conociendo los costos del acceso a determinada información o herramienta.

El análisis planteado en el presente trabajo se realiza enfocando el tema desde el punto de vista del Derecho a la Protección de Datos Personales, dando relevancia a aspectos interdisciplinarios, como conceptos provenientes de la tecnología, base imprescindible a la hora de comprender su regulación y alcances.

Es importante establecer a los efectos de acotar el objeto de estudio, mi concepción particular acerca de la protección de los datos personales en el entendido que considero sumamente importante la defensa de este derecho, en su carácter de derecho fundamental.

Es de rigor destacar que ésta concepción no es unánime, ya que hay muchos defensores de los diferentes sistemas publicitarios, entendiendo que éstos, lejos de perjudicar a los usuarios con intromisiones a su privacidad, acarrean importantes beneficios a la hora de ofrecer productos que pueden ser de su interés, presentando, por ejemplo, ofertas y novedades.

Estudiaremos el marketing comportamental en línea, a través de la trascendencia y regulación de las cookies, pero partiendo de un marco más amplio, desde el marketing electrónico en general y con especial énfasis en los principios y amenazas a la protección de datos personales. Nos referiremos a la

problemática y regulación europea, pero realizando también un análisis del derecho positivo argentino y uruguayo.

# CAPITULO I

# INTRODUCCION AL MARKETING ELECTRONICO

## 1. INTRODUCCION

La información se ha convertido hoy día en un bien jurídico de extraordinario valor, provocando cambios de paradigmas, uno de ellos vinculado al acceso a la información y, al procesar ésta tecnológicamente y circularla a través de las redes telemáticas, se han ocasionado cambios también, en las concepciones de tiempo y espacio.

"Son muchos los que hoy califican a la información como el auténtico poder de las sociedades avanzadas. Los Estados, las asociaciones, las empresas son tanto o más poderosas en cuanto que disponen de grades volúmenes de información. El conocimiento en general y el científico en particular exigen hoy día el procesamiento, el acceso y la valoración de fuentes de información múltiples y diversas"[1].

La tecnología nos permite realizar cualquier tipo de procesamiento de información, obtenerla, modificarla o alterarla, borrarla, ordenarla, difundirla y almacenarla de manera prácticamente ilimitada, tanto de forma legal como ilegal.

"Resulta extraordinariamente sencillo acceder a datos personales como el nombre, apellidos, domicilio, teléfono, fax, dirección de correo electrónico o estado civil que, pudiendo parecer inocuos, al cruzarlos con los hábitos de consumo o al tratarlos con programas "datamining" –dedicados a buscar información sensible escondida dentro de las bases de datos- nos proporcionan, al entrecruzarse como haces de luz, una silueta perfecta que refleja el yo más íntimo del potencial consumidor, perfecta representación de sus tendencias naturales, intuitivas e instintivas. Esta información es extraordinariamente útil para los publicistas que, gracias a la técnica, conocen de manera más fiel el comportamiento de los consumidores"[2].

Las Tecnologías de la Información y Comunicaciones han repercutido en los distintos ámbitos de la vida económica, política, social y también jurídica. El presente trabajo tiene como objetivo principal realizar un análisis del marketing

[1] ALVAREZ-CIENFUEGOS SUAREZ, José María. "La defensa de la intimidad de los ciudadanos y la tecnología informática". Aranzandi 1999. Colección Divulgación Jurídica. Página 13.

[2] PALADELLA SALORD, Carlos. "Datos personales contenidos en bases de datos y registros electrónicos. REDI número 7 de febrero de 1999.

comportamental en línea desde la óptica de la protección de datos personales, partiendo de la pregunta si esta modalidad es invasiva de la privacidad de las personas. Este tema, es un aspecto específico de la publicidad realizado por medios electrónicos y dentro de ésta, la importancia que cobra el marketing.

La globalización condiciona todo el accionar de la economía y de la vida cotidiana en todo el mundo. Ya no podemos pensar de otra manera que globalizada, así nuestro actuar sea exclusivamente local. El actuar de las empresas puede ser local, pero la visión del negocio tiene que ser holística y global. En marketing se emplea el término "glocal" (e-glocal), para definir una estrategia más que un concepto, el de pensar globalmente y actuar localmente. Glocal es un neologismo utilizado por muchos pensadores y autores, entre ellos Beck, U., 1998[3].

Comenzaremos, entonces, analizando el marketing electrónico, su concepción y modalidades.

"Marketing": se trata de una voz inglesa que se ha impuesto en ámbitos de lengua hispana, incluso en literatura especializada. La Real Academia Española traduce el término por "mercadotecnia" y lo define de la siguiente forma:

a. Conjunto de principios y prácticas que buscan el aumento del comercio, especialmente de la demanda.

b. Estudio de los procedimientos y recursos tendientes a este fin.

Entendemos como sinónimos publicidad electrónica, publicidad telemática, actividad promocional on line y comunicaciones comerciales electrónicas. Obviamente este tema, tiene una vertiente muy importante que se centra en el derecho comercial, la publicidad comercial como tal y el derecho de los consumidores desde la óptica de las relaciones de consumo. Y no podemos dejar de mencionar, a nivel Constitucional la libertad de empresa y la libertad de información.

Desde este punto de vista, teniendo en cuenta que el destinatario de un mensaje comercial recibe cierta información de carácter objetivo sobre la entidad o sobre los bienes y servicios de la misma. Este reconocimiento trae como consecuencia la imposibilidad de aplicar arbitrariamente limitaciones a su libre desarrollo más allá de los presupuestos jurídicos exigidos en cuento al contenido de la misma, como es el respeto al principio de veracidad[4].

[3] RIOS, Mauro. "El pequeño empresario en América Latina y el Caribe, las TIC y el comercio electrónico".

[4] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Marcial Pons. Madrid, 2008.

Hay que tener en cuenta que el concepto de "destinatario de la publicidad" es más amplio que el de "consumidor o usuario".

Otros fenómenos ahora incipientes, como el *e-geomarketing* soportado por *bluetooth*, es una modalidad que permite enviar mensajes publicitarios a los terminales telefónicos que estén en el área de alcance del *bluetooth* de un establecimiento, lo que puede analizarse también desde la perspectiva de la protección de la intimidad[5].

La cantidad de bienes materiales vendidos a través de medios electrónicos es cada vez mayor, observa Charles Mc Lure. Este fenómeno abarca todas las transacciones, desde las operaciones tradicionales, por ejemplo, los contactos telefónicos y televisivos llamados "*infomercials*" (mensajes comerciales prolongados, presentados con la forma de informaciones), hasta llegar al marketing on line vía Internet, cuyo elemento más importante está representado por la web[6].

La red Internet es un medio de comunicación polifacético con alcance global, herramienta idónea para las empresas para hacerse conocer y llegar a los diferentes nichos de mercados. Existen diferentes medios para distribuir información, y por lo tanto para realizar marketing electrónico, como por ejemplo el correo electrónico, los boletines, los foros de discusión, los blogs y también la información presente en la www[7].

La publicidad en Internet, además, presenta indudables ventajas frente a la difusión de la publicidad en nuestros medios tradicionales. Así, en primer lugar, es una publicidad más barata. Pero, además de suponer un costo inferior, la publicidad en Internet puede llegar a ser más eficaz que la publicidad en nuestros medios más tradicionales. Gracias a Internet, se puede trazar con precisión un perfil de potencial del cliente y de sus preferencias. Y se puede también, por lo tanto, programar la información que cada cliente potencial desea recibir[8].

La privacidad desinhibe al potencial comprador, contrarrestando las propias cualidades del medio virtual, siendo éste un medio impersonal, frío y sobre poblado de información lo que a todas cuentas, provoca temores, dudas y percepciones diferentes de cada factor ante el cual se enfrenta este individuo.

[5] PEINADO GRACIA Juan Ignacio. Prólogo del libro "La protección de los destinatarios de las comunicaciones comerciales electrónicas" de Trinidad Vázquez Ruano. Marcial Pons. Madrid, 2008.

[6] McLURE, Charles E., Jr. y CORABI, Giampaolo. "La tributación sobre el comercio electrónico: objetivos económicos, restricciones tecnológicas y legislación tributaria". Depalma. Buenos Aires, 2000.

[7] VIEGA, María José. "Privacidad en Internet". Derecho Informático. Tomo II. Año 2001. Fundación de Cultura Universitaria. Montevideo, 2002.

[8] ANXO TATO PLAZA. "Internet, a Publicidade e a Concorrencia" en Temas de Direito da Informática e da Internet. Coimbra Editora. 2004. Página 182.

La estrategias de marketing han sufrido, por lo precedentemente detallado, un revés al tradicionalismo y por lo tanto la realidad dicta que no podemos segmentar el público objetivo por su condición de personas o individuos sino por su psiquis y su singularidad vivencial a la hora de comprar[9].

La tecnología de Internet ha generado una serie de fenómenos de adaptación y cambios en la vida comercial. La Dra. Beatriz Bugallo se refiere a algunos de ellos, como el redimensionamiento o revalorización de la marca para la individualización del comerciante, evocando una experiencia anterior del cliente o usuario para los diversos productos o servicios ofrecidos en Internet, así como los cambios empresariales en los sistemas de distribución debidos a la digitalización de productos o prestación de servicios a través de la digitalización, entre otros. Por otra parte, tanto para el empresario como para el accionista, la gestión de su actividad o intereses comerciales por vía electrónica, a través de Internet, posibilita un mejor contacto y control[10].

Internet cambia los medios de comunicación, permitiendo establecer una comunicación interactiva con los usuarios y una atención personalizada. Los problemas planteados por el comercio, a nivel histórico, por carencia o deficiencia de la normativa que los regulara, fueron resueltos por los propios comerciantes a través de los usos y prácticas consagrados por la costumbre. También se han planteado estos usos comerciales en la sociedad de la información, la autorregulación como forma de solución a las nuevas interrogantes planteadas por la tecnología[11].

La Dra. Beatriz Bugallo[12] distingue tres facetas de la actividad del empresario respecto a las nuevas situaciones que le plantean las tecnologías:

a) frente a sus competidores: se plantean temas relacionados con la lealtad de la competencia, los nombres de dominio, las marcas, los nombres comerciales y denominaciones de origen y también los derechos de autor.

b) frente a los clientes o consumidores: el empresario por Internet debe apoyarse más que nunca en la lealtad y buena fe, toma relevancia la calidad del objeto y el cumplimiento en forma de la prestación, es relevante la particular posición del consumidor internauta, sentado solo frente a la pantalla y con medios tecnológicos que determinan que haya perfeccionado un contrato por el mero "clickeo" de su computadora.

---

[9] RIOS Mauro D. “Des espaldas al Chip. Breves guías de cómo ver la tecnología”. Montevideo, Mayo 2000. Página 93.

[10] BUGALLO, Beatriz. “Nuevos usos en la sociedad de la información”. Conferencia dictada en el Simposio organizado por Antel sobre Ética e Internet, sección "Internet y los cambios de la vida cotidiana". Radisson, 2000. http://beatriz.bugallo.info

[11] DELPIAZZO, Carlos y VIEGA, María José. “Lecciones de Derecho Telemático. Tomo II”. Fundación de Cultura Universitaria. Montevideo, marzo 2009. Página 230.

[12] BUGALLO, Beatriz. “Nuevos usos en la sociedad de la información”. Ob. Cit.

c) en cuanto a su propia gestión comercial y social, interna: el empresario que negocia por Internet cuenta hoy con la posibilidad de reestructurar el sistema de distribución de productos, cuando éstos son digitalizables. Respecto de algunos bienes se puede prescindir del soporte físico que se distribuía y ofrecía en el mundo material. Se habla hoy de los "bienes de Internet" o la "mercadería de Internet" cuando se trata de programas de ordenador, música, libros, entre otros.

La búsqueda de soluciones para el fenómeno de la globalización ha girado en torno a temas como son la ley aplicable y la jurisdicción competente, relacionada con el cambio de paradigma respecto al espacio, la desaparición de fronteras físicas en el ciberespacio y la transferencia de bienes virtuales de un lugar a otro del planeta.

La globalización de sistemas jurídicos diferentes, con precedentes jurisprudenciales diferentes plantea, frente a la globalización un escenario similar al que planteaba la anomia medieval que debió enfrentar el comercio. ¿Cómo se solucionó dicha anomia? Mediante la consolidación de usos a través de la creación de una trama de derecho consuetudinario derivado de los usos y prácticas del comercio conocido y aplicado por los comerciantes que recibió el nombre de "lex mercatoria" y que fue la génesis de la legislación estatal decimonónica - la época de los grandes Códigos. La lex mercatoria se gestó, no apelando a una simbiosis en normas de sistemas existentes, sino aplicando los principios que surgían de la propia naturaleza de las cosas y de la esencia misma del hombre, tamizados por las peculiaridades y necesidades especificas que una actividad profesional especializada como la ley mercantil demandaba. (...) De la misma manera que en la Edad Media se concentraron en distintos documentos los principios generales reguladores del comercio. Asimismo, circulan ya expresiones tales como "Lex Informatica" o "Lex cybernetoria", emulando o reconociendo la lección histórica de la "Lex mercatoria" en la atribución de soluciones jurídicas[13].

Las nuevas tecnologías permiten expandir las actividades de marketing con un alcance mundial, siendo Internet una poderosa herramienta en este sentido. Las páginas web empresariales son uno de los elementos esenciales para la comunicación entre las empresas y los clientes. En esta forma de comunicación podemos destacar como elementos relevantes: la posibilidad de acceso las 24 horas del día, los problemas de medición digital, el grado de mayor interacción, las ofertas ilimitadas, la relación cliente-fabricante[14].

[13] Beatriz BUGALLO. “Nuevos usos en la sociedad de la información”. Ob. Cit

[14] DELPIAZZO, Carlos y VIEGA, María José. “Lecciones de Derecho Telemático. Tomo II”. Ob. Cit., página 231.

Un elemento muy importante a no perder de vista es el crecimiento que está teniendo la publicidad en Internet , sobre todo en la redes sociales.

La Cámara Internacional de Comercio (CIC) actualizó en diciembre de 2004 las directrices sobre marketing y publicidad electrónicos, la que constituye una forma de autorregulación, complementaria de las normas jurídicas existentes.

La edición abarca la publicidad electrónica, las comunicaciones interactivas, como Internet, los servicios en línea interactivos y las redes de comunicación electrónica, incluido el teléfono. Entre sus objetivos está, entre otros, elevar el nivel de confianza del público consumidor en el marketing y la publicidad electrónica; garantizar un nivel adecuado de privacidad para los consumidores, respetar las preferencias del público; y salvaguardar la libertad de expresión de comerciantes y publicistas. Con la presentación de estos códigos de conducta la CIC pretende ofrecer soluciones prácticas y flexibles, y reducir la necesidad de acudir a la vía de las medidas legislativas gubernamentales e Inter-gubernamentales[15].

En estas circunstancias, creemos que la red también debe dejar un cierto incremento de nivel de responsabilidad y autotutela a los consumidores. En gran medida, son estos consumidores los que deberán aprender a discriminar la información que merece su confianza de la que no. Si Internet equivale a la aldea global, es evidente que las autoridades deberán velar por la seguridad de la aldea, pero los consumidores también deberán iniciar un proceso de aprendizaje que les permita distinguir que calles de la aldea son seguras y que calles por el contrario son peligrosas[16].

## 2. HERRAMIENTAS Y PRINCIPIOS DEL MARKETING ELECTRONICO

No dejan de sorprenderme las diferentes herramientas que la red da a los anunciantes para realizar sus actividades de marketing, las cuales tienen ciertos principios, que entiendo vale la pena considerar.

### 2.1 El sitio web

Según Daniel Amor[17] una estrategia de marketing en Internet debe respetar las siguientes reglas:

- Marcas: el sitio web de la empresa es la marca más importante.

[15] www.iprhelpdesk.org/controlador.jsp?cuerpo=noticiasCuerpo&seccion=noticiaseventos&tipoListado=all&id=0000005588&len=es Página visitada 1 de mayo de 2005.

[16] DELPIAZZO, Carlos y VIEGA, María José. "Lecciones de Derecho Telemático. Tomo II". Ob. Cit., página 232.

[17] AMOR Daniel. "La (R)evolución. E-business. Claves para vivir y trabajar en un mundo globalizado". Prentice Hall. Buenos Aires, 2000. Página 134.

- Cambio: las reglas de Internet están cambiando.
- Concisión: genere páginas cortas con la información distribuida en varias páginas.
- Contenido: el contenido es el que manda, no hay que aburrir a los clientes.
- Sitios dinámicos: cree sitios que empleen nuevas tecnologías para adaptar información sobre la base de perfiles de usuarios.
- Finanzas: incursione en nuevos mercados con programas de precios de publicidad accesibles.
- Promociones con regalos: arme ofertas con regalos para los clientes fieles.
- La Aldea Global: piense en términos globales, pero actúe en términos locales.
- Eventos en vivo: los eventos on-line sirven para generar rápidamente una conciencia de la empresa en los clientes.
- Nichos: Internet es una serie de nichos y mercados masivos.
- Promoción: promocione su sitio en todas partes.
- Formación de sociedades: únase con otras empresas para promocionar sus productos y servicios.
- Tecnología: debe emplearse la tecnología de Internet para maximizar los objetivos de marketing.

Ahora bien, ¿cómo se atraen visitantes al sitio? Daniel Amor –citado con anterioridad- realiza una serie de recomendaciones:

a. En primer lugar el sitio debe estar actualizado para que los usuarios regresen para ver noticias e informaciones.

b. Es importante también ofrecer información, productos y servicios gratuitos para quienes visitan el sitio.

c. La personalización es importante, cuanto más sepa de los usuarios de su sitio, mejor podrá desempeñar su tarea de marketing.

Y este es el punto neurálgico en nuestro trabajo, ya que este "conocimiento" del cliente no debe convertirse en una violación de su privacidad, sino que los datos deben ser obtenido con su previo consentimiento informado, y sobre este principio volveremos una y otra vez, ya que constituye una columna fundamental en la defensa de la protección de los datos personales.

d. Por otro lado los sorteos son muy atractivos para los clientes.

e. Es fundamental proteger la privacidad de los clientes e informarles acerca de la política de la empresa al respecto, lo que se hace a través de los términos legales del sitio.

   Pero, en nuestra opinión, en la mayoría de los casos, esos "términos legales" se convierten en una autorización para que la empresa utilice la información personal, amparada en ellos y se exonere de responsabilidades de todo tipo de usos. Por tanto, las condiciones legales del sitio web deben guardar un equilibrio entre los intereses de la empresa y los derechos de los consumidores.

f. La posibilidad de realizar impresiones que no tengan formato web es de utilidad para los usuarios. Es importante anticiparse a las necesidades del cliente, por lo que la creación de referencias cruzadas entre productos y servicios es muy útil. Este tipo de prestación es muy usada en las librerías on line, en las cuales cuando usted adquiere un libro se le presentan otros libros del mismo autor o tema, o bien libros que otros clientes compraron tras adquirir ese libro en particular.

   Aquí tenemos la primer referencia "positiva" a las cookies, ya que este tipo de servicios se logra con su instalación. Y vemos que si bien hoy las cookies nos presentan ciertos desafíos y se han convertido en un tema de preocupación y discusión, ellas han venido conviviendo con nosotros hace ya unos cuantos años, pasando desapercibidas para la mayoría de los usuarios. Creo que el abuso de las mismas, y no la prestación de un simple servicio, es lo que las ha llevado hoy al protagonismo que detentan.

g. El marketing de eventos también atrae nuevos usuarios y retiene a los existentes, pudiendo muchas veces suscribirse a *mailing lists* para comunicarles los eventos en los que pueden participar.

## 2.2 Asociaciones con otras empresas

Es importante en Internet, a los efectos de colocar productos o servicios, asociarse con otros sitios u otros medios. Los portales, por ejemplo, son una buena herramienta para ofrecer productos o servicios.

Redes afiliadas: constituyen una forma especial de personalizar los productos en línea, en este caso no para los clientes finales, sino para los revendedores que desean expandir sus ofertas agregando servicios, productos o información. (...) Otra razón para crear una red afiliada es la generación de una conciencia de marca[18].

Comunidades virtuales: el armado de comunidades dentro del sitio le permitirá conocer mejor a sus clientes y efectuar estrategias de *marketing one-to-one*. La política de privacidad será aquí relevante para tener la confianza de los miembros.

En este punto aparecen dos aspectos de interés a ser analizados posteriormente, por un lado, el clásico "es importante conocer al cliente" y lo que esto implica y por otro, las asociaciones y redes que como veremos, dan origen a la existencia de cookies de terceros, no del propietario del sitio web que las instala, sino de un socio que realmente es quien procesa la información.

## 2.3 Mediciones on line

Los principales métodos de medición utilizados en la Web son: el recuento, la auditoría y el rating[19].

El recuento es el proceso que habitualmente realizan los dueños de los sitios.

La medición se basa en los archivos del registro del servidor web, que se procesan para enviar cifras procesadas a los anunciantes. Dado que las cifras se basan en el archivo de registro de un sitio en especial, los anunciantes no pueden saber si los datos son comparables entre sitios diferentes[20].

Los anunciantes pueden registrarse en agencias de rating on line. Estas agencias utilizan un software especial que monitorea la actividad de los clientes y que se debe instar en la computadora de cada usuario. La tecnología es similar a los servicios de rating de televisión.

[18] AMOR Daniel. "La (R)evolución. E-business. Claves para vivir y trabajar en un mundo globalizado". Ob. Cit., página 148.
[19] DELPIAZZO, Carlos y VIEGA, María José. "Lecciones de Derecho Telemático. Tomo II". Ob. Cit., página 234.
[20] AMOR Daniel. "La (R)evolución. E-business. Claves para vivir y trabajar en un mundo globalizado". Ob. Cit., página 164.

Existen diferentes formas de realizar la medición, a través de: visualización de página; visitas realizadas por un solo visitante, la cual se da por finalizada si el usuario no mira la página por 15 segundos, solicitud: cada acceso a un servidor web , usuario que puede identificarse ya sea a través de la dirección de e-mail o a través de las cookies, cantidad de vistas de banners en una página, cantidad de clics en un *banner* en una página. Se habla de clics reales cuando el usuario cliquea en el banner y es llevado al sitio determinado por el anunciante.

Pero los sistemas de mediciones no son exactos, se basan en estadísticas, y pueden variar por diferentes razones, como por ejemplo el almacenamiento en caché de un sitio, o cuando se producen errores de descarga de los gráficos, o la comunicación es lenta, el servidor computa la página como visualizada, pero el usuario nunca llegó a ver la imagen. También ocurre que voluntariamente el usuario interrumpa la descarga, para ver otra cosa, o ir hacia atrás, etc., antes que el anuncio se descargara totalmente. Y por supuesto, muchas veces no prestamos atención a los anuncios, porque no nos interesa.

## 2.4 Marketing one-to-one

Es el marketing por excelencia en la Web. Debe utilizarse la identificación, interacción, diferenciación, seguimiento y personalización, haciéndolo en forma combinada para tener éxito en el marketing por Internet[21].

La identificación permite conocer al cliente, de forma tal que a través de la interacción podrá ofrecérsele productos o servicios que sean de su interés. En virtud de las características del cliente se le va a ofrecer productos diferenciados.

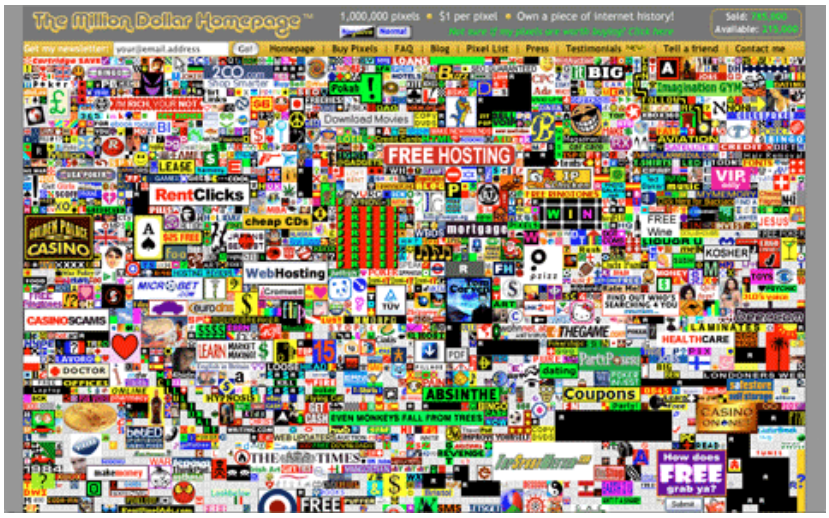
A través del seguimiento de las transacciones que realiza se va a comprender mejor cuales son sus gustos y/o necesidades. La personalización se da a través de ofrecer módulos de productos, información de servicios que se adapten en forma específica a las necesidades de cada cliente.

## 2.5 Formas innovadoras de Marketing en la web

Como mencionaba al inicio, la creatividad en esta área es asombrosa, en el buen y mal sentido, tenemos así casos como el de Millon Dólar Homepage, el marketing viral o los pagos por leer publicidad.

[21] VIEGA, María José. “e-Marketing”. Ponencia presentada y publicada en las Memorias del XI Congreso Iberoamericano de Derecho e Informática. Panamá, 19 al 23 de junio de 2006.

Alex Tew, de 21 años, encontró una original idea para poder financiar sus estudios. Su idea se llama *The Million Dollar Homepage*[22], y consistió en vender publicidad a 1 dólar por pixel, ofreciendo un total de 1 millón de píxeles. El espacio más pequeño a la venta fue un bloque de 10 x 10 píxeles, a un precio de 100 dólares.




Esta idea ha llevado a que otros lo intenten, con publicidad relacionada a determinado rubro, así es que tenemos sitios como, a vía de ejemplo: million dólar woman[23], million dólar penny[24]. También hay quienes han realizado modificaciones a la idea original, como AlquilaTuPixel.com, página en la cual en lugar de vender los pixeles se alquilan por un año a un céntimo de dólar cada píxel[25].

Desde el punto de vista de la protección de datos personales este sistema es inocuo para quien contrata el tablón de anuncio.

Por otra parte, una estrategia de marketing viral consiste básicamente en conseguir que los usuarios se transmitan los unos a los otros un determinado mensaje, noticia, promoción, evento, etc., obteniendo de este modo un crecimiento exponencial del alcance de este. Marketing viral significa la creación de mensajes que incluyen un concepto dentro de el que es absorbido por la gente que entra en contacto con él. Y dicho mensaje es tan bien aceptado que las personas empiezan a transmitírselo unos a otros[26].

---

[22] www.milliondollarhomepage.com Página visitada el 13 de enero 2006.
[23] http://www.milliondollarwomenshomepage.com Página visitada el 13 de enero 2006.
[24] http://www.millionpennyhomepage.com Página visitada el 13 de enero 2006.
[25] http://dhost.info/veducm/alquilatupixel/index.htm Página visitada el 2 de diciembre de 2006.
[26] Material del Master Universitario "Asesoría Legal en Tecnologías de la Información". Curso on line de la Universidad Politécnica de Valencia. Tema: "Marketing y Publicidad en Internet". Marzo 2005.

Un ejemplo de ello es el caso Hotmail, cuando un usuario enviaba un mensaje, al final del mismo aparecía "*Get Your Private, Free E mail from* MSN Hotmail a http://www.hotmail.com". De manera que quien recibía un mensaje se registraba y a su vez los mensajes que enviaba éste también tenían la leyenda que era distribuida a nuevos usuarios.

Por último, no quiero dejar pasar la existencia de los llamados "pagos por leer publicidad", porque estos sistemas, bajo el título de "trabajo on line", lo que hacen es publicidad sobre un sistema de venta piramidal, llevando a incautos a adquirir determinados productos, tales como tarjeta de pertenencia a un círculo de socios o círculo dorado, etc. que le permitirá ganar mucho más por la lectura de cada mensaje publicitario. Además, debe conseguir personas que adhieran a su pirámide para poder ganar sobre los que ellos leen. Para que le paguen, debe adquirir una determinada tarjeta, que tiene un costo anual determinado[27].

## 2.6 Marketing directo

Se puede definir como toda comunicación cuantificable, cualificable y previsible, efectuada por cualquier medio conocido o por conocer, que tenga por objeto principal crear y explotar una relación directa a distancia entre una empresa y/o un individuo y sus clientes o prospectos, tratándolos individualmente. Se consideran actividades de Marketing Directo la generación de tráfico hacia instalaciones físicas y la generación de "leads" (oportunidades de venta) para vendedores físicos, siempre que el estímulo utilizado en generar el tráfico/lead incluya un contacto por medios masivos, correo, teléfono o email/Internet u otro medio por conocer.

El marketing directo está ampliamente integrado en todos los medios publicitarios e incluye correo directo, telemarketing, televisión, radio, periódicos, revistas y, naturalmente Internet. Creemos que la forma de telemarketing directo más comparable a Internet es el correo directo[28].

En el marketing directo se utilizan herramientas como el correo electrónico, *mailing list* y los boletines informativos. El titular de la empresa tendrá que tener cuidado de no caer en el abuso en el envío de mail, con lo cual se convierte en spam, lo que termina molestando al cliente. Además, hay que ser cuidadosos de que el mensaje tenga valor para el cliente.

[27] DELPIAZZO, Carlos y VIEGA, María José. "Lecciones de Derecho Telemático. Tomo II". Ob. Cit, página 238.
[28] MEEKER, Mary. "La publicidad en Internet". Ob. Cit., página 125.

Hay que tener presente la ausencia de fronteras de Internet, debiéndose pensar en un mercado global, pero adaptar el sitio al mercado local, teniendo en cuenta las costumbres de cada lugar, el idioma y las formas de negociación en general.

Es necesaria la utilización del *marketing one-to-one* para conocer a los clientes, pero en este proceso la confidencialidad de la información brindada por el cliente es sumamente importante.

El *direct marketing* de bienes materiales es eficaz en particular si se cumplen ciertas condiciones. Cuando se trata de productos estandarizados, como por ejemplo, automóviles, computadoras y sus componentes periféricos, software, libros y vinos, el cliente puede concentrarse en la búsqueda del precio y de la disponibilidad de los bienes, los cuales son informaciones fáciles de localizar en Internet. La fidelidad del consumidor a una marca determinada ayuda a no alejarse, durante la búsqueda, del objetivo de la compra. La reputación de la integridad del vendedor es importante no sólo como garantía de calidad, sino también como garantía frente al riesgo de entregarle datos de la tarjeta de crédito y para gozar de la posibilidad de devolución de las mercaderías[29].

## 2.7 Marketing interactivo

También denominada publicidad interactiva, consiste en la utilización de medios interactivos para incentivar a los consumidores a realizar una compra. Este sistema se utiliza a través de Internet, de la televisión interactiva y de la telefonía móvil.

El consumidor pasa de tener una actitud pasiva a una activa, pudiendo elegir entre diferentes opciones, solicitar información, entre otras, realizándose un proceso de comunicación bidereccional.

Según Gonzalo Iruzubieta: “La publicidad interactiva está abierta a cualquier tipo de anunciante, y tan sólo es preciso superar ciertas barreras de confianza que quizá se deban a diferencias generacionales”. IAB SPAIN ya engloba a más de un centenar de organizaciones de diversa índole lo que da idea de su pluralidad entre agencias interactivas y de medios, soportes, redes, buscadores, consultoras, medios de comunicación, proveedores tecnológicos. Ahora el reto es luchar contra el cambio generacional y convencer a los grandes directores de marketing de las empresas del valor añadido de la publicidad online[30].

[29] McLURE, Charles E. y CORABI, Giampaolo. “La tributación sobre el comercio electrónico: objetivos económicos, restricciones tecnológicas y legislación tributaria”. Ob. Cit.

[30] IRUZUBIETA, Gonzalo. Director de Marketing y Comunicación de IAB SPAIN. “Debemos fomentar siempre el marketing interactivo en todas nuestras actuaciones”. Diario digital de marketing y publicidad en español. Puromarketing. 14 de octubre del 2008.

El 62% de las reclamaciones tramitadas por la Secretaría de Confianza Online sobre compras electrónicas y publicidad interactiva, se resuelven en un plazo no superior a 10 días mediante un acuerdo de mediación online. La posibilidad de acudir a este sistema extrajudicial de resolución de controversias gratuito, rápido y eficaz, reconocido por la Comisión Europea, es una de las ventajas que tiene el consumidor que accede a una página web que incluye el Sello de Confianza Online (www.confianzaonline.es), un distintivo que permite identificar a las entidades que cumplen toda una serie de requisitos éticos y legales, recogidos en el Código Ético de Confianza Online. Actualmente, son cerca de 500 entidades adheridas las que ya han sido acreditadas con este Sello, que pretende aumentar la confianza de los consumidores en el comercio electrónico y la publicidad interactiva y garantizar la protección del menor, la accesibilidad y usabilidad, así como la protección de datos[31].

Otra expresión que resume la comunicación comercial de nuestros días es un término que ha llegado a calar en el ámbito profesional: Marketing Relacional. Una consideración del Marketing que establece como objetivo prioritario la construcción de una relación (personal) con sus públicos. Desde el punto de vista académico, se habla de un cambio de paradigma, de la sustitución del marketing transaccional al marketing relacional. Las cuatro P s dejan paso a las cuatro C s (Cliente, Características, Canal y Comunicación)[32].

También se está desarrollando el llamado "neuromarketing" por dos investigadores de la Universidad de Duke y la Universidad de Emory, tiene herramientas de la ciencia moderna, como la resonancia magnética funcional, y se aplica para analizar los gustos y disgustos de los clientes en la toma de decisiones. Aunque esto aumenta el espectro de la capacidad de los vendedores de leer las mentes de las personas (más de lo que ya lo hacen), el neuromarketing puede llegar a ser una forma asequible para los vendedores para obtener información que antes era inalcanzable[33].

[31] http://www.autocontrol.es/pdfs/NP%20Asociacion%20Confianza%20Online.pdf Página visitada 12 de junio de 2010.

[32] VICTORIA MAS JUAN Salvador. "Introducción a la comunicación interactiva. La Publicidad como ejemplo del Nuevo Paradigma de la Comunicación. Capítulo del libro Consumidores y usuarios ante las nuevas tecnologías. Lorenzo Cotino Hueso (coordinador). Derecho y tic's. Valencia, 2008. Página 467.

[33] BRINN, Laura. "Brain Scans Could Be Marketing Tool Of The Future. The may nor replace the focus group, but could reveal new information". Thurday, March 4, 2010. www.dukenews.duke.edu/2010/03/brainscan.html Página visitada el 14 de junio de 2010.

# CAPITULO II

# PROTECCION DE DATOS: AMENZAZAS Y PUBLICIDAD

## 1. INTRODUCCION

Cuando pensamos en la problemática y en los desafíos que el ciberespacio plantea, nos encontramos con algunos elementos que podemos calificar como nuevos. Pero en realidad Internet, a redimensionado problemas tradicionales, que si bien estaban regulados jurídicamente, dicha regulación deberá ser actualizada, si es que ya no lo ha sido, para incluir esas nuevas facetas que las tecnologías nos plantean.

Analizaremos en este capítulo la cuestión del derecho a la intimidad, teniendo en cuenta los riesgos personales que plantean los grandes bancos de datos personales, conocidos como "Big Data" y la posibilidad del entrecruzamiento de la información que contienen.

El derecho a la intimidad ha evolucionado hacia un nuevo concepto: la privacidad, la cual se ve seriamente violentada por las nuevas tecnologías, al punto tal que se ha llegado a hablar de la existencia de un hombre de cristal[34].

"Las posibilidades tecnológicas de conseguir un "ciudadano de cristal" son cada vez más grandes, no sólo en el ámbito del manejo de datos sensibles de carácter tradicional (como la filiación política, la pertenencia sindical, la confesión religiosa, el grupo humano al que se pertenece, las costumbres sexuales, las apetencias personales y sociales, el historial clínico y penal, las cuentas bancarias, la situación económica, los viajes, etc.) sino también mediante la digitalización de información genética, lo que permitirá crear un cuadro completo de los aspectos más íntimos de la constitución física, hereditaria y hasta psicológica de alguien. Además, su personalidad puede hacerse transparente para fines de mercado (como para establecer pautas de consumo, etc.) u otras pudiendo llegar a generar una auténtica "estigmatización electrónica"[35].

La privacidad es un tema que puede ser enfocado desde múltiples ópticas, desde el cruzamiento de ficheros en soporte papel, el de ficheros electrónicos,

[34] VIEGA, María José. "Protección de datos y delitos informáticos". Ponencia presentada al III Congreso Internacional de Derecho. Bolivia, 10 al 13 de setiembre de 2003 y publicada en el Libro de Memorias de dicho Congreso.

[35] DELPIAZZO Carlos. "Dignidad Humana y Derecho". Universidad de Montevideo. Facultad de Derecho. Montevideo, 2001. Página 124.

la privacidad desde la óptica del consumidor y de las telecomunicaciones (sean por cable o inalámbricas) y nuestro tema de hoy, son las connotaciones en el ámbito de Internet[36].

Se ha calificado a Internet como una amenaza en la difusión de elementos relativos a la persona, por ser un medio masivo y polifacético de comunicación. Tal es así, que hemos analizado en otra oportunidad[37] las diferentes clases de comunicaciones a través de la Red y las hemos comparado con las comunicaciones "tradicionales", estudiando similitudes y diferencias con la correspondencia privada, la prensa escrita y la radiodifusión.

Para comenzar a reflexionar sobre este tema me gustaría que pensáramos sobre las siguientes preguntas: ¿Hay alguien escuchando nuestras llamadas telefónicas? ¿Alguien lee nuestros mail? ¿Y nuestros chat? ¿Es posible que alguien recupere a través del proveedor lo que escribimos hace unos meses? ¿Es realmente importante la privacidad para cada uno de nosotros?

En los hechos, la mayor parte de las personas ceden sus datos a cambio de puntos, millas, etc. sin tener conciencia que nos estamos identificando, que estamos dando información sobre nuestros hábitos, consumo, y no conocemos la utilización posterior que se realizará con los mismos.

Ahora bien, ¿"alguien" nos espía? Según el diccionario de la Real Academia Española, espía es una persona que con disimulo y secreto observa o escucha lo que pasa, para comunicarlo al que tiene interés en saberlo.

Si nos preguntamos ¿quién nos espía a través de Internet? La respuesta será los Gobiernos, las empresas y los ciberdelincuentes.

¿Para qué nos espían? Depende de la respuesta que demos a la pregunta anterior serán los motivos. Los gobiernos en aras de la seguridad nacional, las empresas buscan crear perfiles de usuarios a los efectos de ofrecernos productos que sean de nuestro interés, lo que tendrá como resultado el spam, también existe el espionaje entre empresas, el cual se traduce como competencia desleal, y los ciberdelincuentes obviamente desean obtener nuestros datos para obtener un beneficio económico con la utilización de los mismos.

Y una pregunta fundamental es ¿cómo nos espían?

---

[36] VIEGA, María José. "El problema de los datos personales y el espionaje en Internet". Cuarto Congreso Internacional de Derecho (CIDER 2005) en las Sedes de Cochabamba, Santa Cruz y La Paz. Bolivia, 23 al 25 de noviembre de 2005. Publicada en el Libro de Ponencias.

[37] VIEGA, María José. "Derechos Humanos en el Ciberespacio". Trabajo publicado en la Revista electrónica de Derecho Informático (REDI). Junio de 2002.

"En el pasado, si el Gobierno quería violar la privacidad de los ciudadanos tenía que dedicar una cierta cantidad de esfuerzo para interceptar, abrir al vapor y leer el correo de papel. Esto es similar a pescar con una caña, un pez cada vez. Afortunadamente para la libertad, esta vigilancia que requiere tanto esfuerzo no es práctica a gran escala. Hoy en día, el e-mail está reemplazando al correo convencional y, a diferencia de éste, los mensajes electrónicos son facilísimos de interceptar y escudriñar buscando palabras clave. Esto se puede llevar a cabo de manera rutinaria, automática, indetectable y a gran escala. Es similar a la pesca con red de arrastre, lo que constituye una diferencia orweliana para la salud de la democracia"[38].

George Orwell escribió una novela en el año 1948 de ciencia ficción titulada "1984" en la cual nos presenta el mundo del futuro dividido en tres estados totalitarios. El protagonista es el símbolo de la rebelión contra el poder de un estado policíaco (bajo el control del Gran Hermano) que ha llegado a apoderarse de la vida y la conciencia de todos sus súbditos, interviniendo en las esferas más íntimas de los sentimientos humanos[39].

Si quien nos espía es el Estado, la pregunta relevante es: ¿estamos dispuestos a "perder" nuestra intimidad, nuestra privacidad debido a la Seguridad Nacional, de nuestro o de un tercer país. ¿Cuáles son los límites? ¿Somos concientes de los alcances?

## 2. AMENAZAS A LA PRIVACIDAD EN INTERNET

A los efectos de buscar una protección en torno a este tema, tenemos que ponderar dos intereses diferentes, por un lado la protección de la vida privada y por otro el interés de la sociedad toda en que circule cierta información.

Internet entonces, nos replantea el desafío a los efectos de la protección de los datos personales, desafío que se originara a raíz del proceso de informatización de las bases de datos, convirtiendo los ficheros manuales en electrónicos, haciendo posible el relacionamiento de los mismos, así como el cruzamiento de bases de datos, a los efectos de lograr un perfil lo más acabado posible acerca de un individuo.

La Red es un medio de comunicación polifacético, debido a la existencia de múltiples medios para distribuir información. Ellos son: el correo electrónico, los boletines, los foros de discusión y también la información presente en la www[40].

[38] ZIMMERMANN, autor del paquete criptográfico PGP, citado por García Mostazo Nacho en "Libertad Vigilada. El espionaje de las comunicaciones". Ediciones B. Barcelona, 2003.
[39] ORWN George. 1984. Ediciones Destino. Barcelona. Séptima edición, junio 1984.
[40] VIEGA, María José. "Privacidad en Internet". Derecho Informático. Tomo II. Fundación de Cultura Universitaria. Montevideo, 2001.

## 2.1 Herramientas de uso básico

Para enfrentar este desafío debemos tener en cuenta los siguientes elementos[41]: el hecho que la infraestructura de Internet esté basada en datos personales, las nuevas formas de distribuir información, también los instrumentos técnicos utilizados son nuevos y la información utilizada para las actividades en líneas. Estos temas los analizaremos más adelante con mayor detenimiento.

## 2.2 Software de espionaje

Existen también diferentes software diseñados específicamente para obtener información personal, como ha sucedido en Estados Unidos, país sobre el que podemos decir que, con carácter general, se ha buscado la protección a través de la autorregulación y el sistema funciona en base a los principios de puerto seguro.

¿Pero qué sucede con el espionaje de las comunicaciones? Afirma Nacho García que[42]: "las agencias estatales de espionaje siempre han tratado de obtener información a través del llamado espionaje humano (Human Intelligence, Humint), es decir, utilizando a agentes infiltrados. Sin embargo, hay otros sistemas técnicos para llevar a cabo esta misión. Se trata de la inteligencia de señales (Signals Intelligence, Sigint[43]), actividad que consiste en obtener información interceptando las señales electromagnéticas del país objeto de espionaje, sean cuales sean esas señales. Dentro de la actividad del Sigint, una de las facetas más importantes es el espionaje de las comunicaciones (Communication Intelligence, Comint), que consiste en interceptar sólo aquellas trasmisiones que transporten información mediante la interceptación de comunicaciones extranjeras por personas distintas a las que esa información va dirigida.

A partir de 1970, ante la abundancia de información interceptada, programaron computadoras para que las propias máquinas seleccionaran las comunicaciones realmente interesantes, descartando el resto. Este proyecto

[41] ARAGON REYES, Manuel y FERNANDEZ ESTEBAN, María Luisa. Incidencia de Internet en los Derechos Fundamentales. Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid)

[42] GARCIA MOSTAZO, Nacho. "Libertad vigilada. El espionaje de las comunicaciones".Ob. Cit., página 16.

[43] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/04-01.htm Directiva número 6 del Consejo de Seguridad Nacional sobre Inteligencia (NSCID nº 6). "La Agencia de Seguridad Nacional y el Servicio Central de Seguridad".Departamento de Defensa de Estados Unidos, 23 de diciembre de 1971.

recibió el nombre de Echelon, que en español puede traducirse como "escalafón", "escalón" o "grado". Los ordenadores contaban con un "diccionario" de palabras clave para buscar entre los mensajes interceptados y entresacar sólo aquellos que contuvieran las citadas palabras. Cada "diccionario" se actualiza regularmente con las llamadas "listas de vigilancia", que iban cambiando en función de las necesidades de información de los gobiernos implicados en la trama de espionaje global[44].

En 1998 nace Echelon II, como una ampliación de la primera. La Agencia de Seguridad Nacional contrató –entre otros- al ingeniero Bruce McIndoe. En 1998, fecha en que Bruce McIndoe abandonó la NSA, Computer Sciences Corporation (empresa contratada por la NSA) concluyó el proyecto para crear Echelón II, lo que coincide con la puesta en funcionamiento de la "máquina de transcripción de la voz humana", ya que la Agencia de Seguridad Nacional solicitó su patente en 1997[45].

La Agencia de Seguridad Nacional no está autorizada para espiar a ciudadanos norteamericanos porque la ley se lo impide. Pero quien puede hacerlo es la Oficina Federal de Investigación (FBI), cuya jurisdicción se circunscribe al interior de las fronteras norteamericanas.

En los años 90 el FBI desarrolló un programa llamado "Carnivore" capaz de hacer el seguimiento de un usuario a través de la Red.

En 1994 el Congreso de Estados Unidos aprobó la Ley de Asistencia en Comunicaciones para los Cuerpos de Seguridad (Communications Assistance for Law Enforcement Act, CALEA)[46]. Se establece en esta norma la obligación legal de los operadores de telecomunicaciones y los fabricantes de equipos informáticos de incluir dispositivos de vigilancia en toda la red telefónica de Norteamérica.

Carnivore se instaló a partir de abril del 2000 en los Proveedores de Servicios de Internet (ISP), se desveló la existencia del mismo por la oposición de una empresa a instalarlo. Como consecuencia el programa cambió de nombre y se le denominó DCS1000 Digital Collection System (Sistema de Recolección Digital)[47].

Otro programa es el llamado "Linterna Mágina" que se desarrolló durante el año 2001. Este troyano podría enviarse a cualquier sospechoso, como un adjunto a

---

[44] GARCIA MOSTAZO, Nacho. "Libertad vigilada. El espionaje de las comunicaciones". Ediciones B Grupo Z. Barcelona, enero 2003. Página 18.

[45] GARCIA MOSTAZO, Nacho. "Libertad vigilada. El espionaje de las comunicaciones". Ob. Cit. Página 116.

[46] www.askcalea.net Página visitada el 13 de junio 2005.

[47] http://facultyweb.maconstate.edu/jashford/Class%20projects/6pmclass/CarnivorePaperandQuestions.doc "Carnivore: The FBI's Email Sniffer".

un mensaje aparentemente inocente. Aprovechándose de algunas vulnerabilidades, podría incluso instalarse sin el conocimiento del destinatario, y a partir de allí capturaría las contraseñas usadas por el supuesto terrorista, enviándolas a las oficinas del FBI.

Linterna Mágica sería parte de un programa más complejo de vigilancia, llamado Cyber Knight (Caballero cibernético), el cuál incluiría una base de datos que permitiría al FBI cruzar información proveniente de e-mails, salas de chat, mensajeros instantáneos tipo ICQ y llamadas telefónicas por Internet. Algunas fuentes consultadas del FBI, ni negaron ni admitieron la noticia, pero declararon que no es nada nuevo que la organización ha estado trabajando con especialistas de la industria de la seguridad, para crear una herramienta que fuera eficaz en combatir tanto al terrorismo, como a otros actos delictivos. Y aunque no debería ser una sorpresa, tampoco es apropiado que se revelen las tecnologías que específicamente se usarán[48].

Las "puertas traseras" que tienen determinados software también son formas de obtener información de los usuarios que utilizan dicho sistema. Un ejemplo de esto fue el caso de Lotus Notes, descubierto por el gobierno sueco en 1997. Se decía que los navegadores fabricados por Microsoft y Netscape tenían incorporados estos sistemas.

El espionaje electromagnético se basa en el hecho de que cualquier aparato eléctrico o electrónico desprende campos electromagnéticos involuntariamente cuando está en funcionamiento. Por lo cual con una antela direccional, un osciloscopio, un sintonizador especial y otros dispositivos capaces de captar y reconstruir a distancia por ejemplo los caracteres que estoy tipiando en un computador.

¿Es verdad que nos espían? La Comisión de la Unión Europea encargada de determinar la existencia de una red de espionaje de comunicaciones de EEUU llamada Echelon, entregó un informe afirmativo al respecto[49]. El informe de Duncan Campbell "Interception Capabilities 2000"[50] se presentó ante el Parlamento Europeo el 22 de febrero de 2000 en sesión abierta a la prensa demostrando la existencia de Echelon, una red mundial de espionaje de las telecomunicaciones.

Los acontecimientos del 11 de setiembre de 2001 en Estados Unidos han llevado a que este país pretenda un estricto control sobre Internet. El gobierno de Estados Unidos no sólo se propone controlar Internet, incluyendo por

[48] LOPEZ, José Luis. "El FBI y sus troyanos". http://www.vsantivirus.com/22-11-01b.htm Página visitada 13 de junio de 2005.
[49] http://www.larazon.es/lared/laredesoias.htm y El Parlamento europeo reconoce la existencia de la red de espionaje Echelon. http://idg.es/pcworld/noticia.asp?id=18239.
[50] CAMPBELL, Duncan. "Interception Capabilities 2000". http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm

supuesto los correos electrónicos, sino que también a solicitado a la Unión Europea, en la carta que se enviara el 16 de octubre, se reconsidere la legislación existente en materia de protección de datos. Se aprobó en el Senado la ley "Combating Terrorism Act of 2001, el 13 de setiembre de 2001, que multiplica las posibilidades de monitorización de las comunicaciones.

Respecto al programa Carnivore en enero de 2005 apareció la siguiente noticia[51]: "El Gobierno de EEUU ha abandonado el uso de un programa especial de vigilancia por Internet concebido para leer mensajes electrónicos y otras comunicaciones entre presuntos criminales, espías y terroristas, se informó hoy. La Oficina Federal de Investigaciones (FBI) ha informado al Senado y la Cámara de Representantes del abandono de ese sistema y de que ahora utilizará programas informáticos comerciales para revisar el tráfico informático en el marco de sus investigaciones".

Los países del tratado UKUSA (Acuerdo secreto firmado en 1948 entre Estados Unidos y Reino Unido, al que adhirieron Canadá, Australia y Nueva Zelanda, entre otras naciones) no son los únicos que lanzaron satélites de espionaje, pincharon cables o instalaron bases para interceptar las comunicaciones de otras naciones. También Alemania, Francia, Israel y Rusia tienen sus sistemas de vigilancia.

## 2.3 Spyware

El "spyware" es una de las formas de espionaje en Internet, son programas que se ocultan en los ordenadores de los usuarios y controlan sus actividades. Este tipo de espionaje puede debilitar la potencia del ordenador, averiar la máquina y presentar a los usuarios una gran cantidad de anuncios no solicitados. El objetivo puede ser obtener contraseñas, números de tarjeta de crédito y otros datos de valor.

El problema del espionaje es el hecho de lograr que los consumidores tomen conciencia ya que como las actividades no son visibles como otro tipo de amenazas 'online' no se les presta la atención necesaria o no se toman medidas adecuadas.

Por ejemplo el 'spam' es molesto y por eso es importante combatido, a pesar que no es peligroso como lo es el espionaje.

Existen algunos programas que han sido etiquetados como "spyware", pero pueden ser inofensivos, e incluso pueden ayudar al internauta. Muchos programas populares como Kazaa y Morpheus, que permiten a los usuarios

[51] http://www.noticiasdot.com/publicaciones/2005/0105/2001/noticias200105-24.htm Página visitada jueves 20 enero 2005.

copiar música y películas de los discos duros de otros vienen con aplicaciones, sirven anuncios 'pop-up' y otras herramientas de marketing como una forma de subvencionar costes. Los programas "Adware", que pueden instalarse gratuitamente pero incluyen anuncios, como WhenU, no recopilan información personal de los consumidores, según varios ejecutivos, y los usuarios pueden retirarlos con facilidad si lo desean[52].

Los pop up son ventanas de Internet vinculadas de forma independiente a una página web, y utilizados como soporte de un mensaje publicitario o como web de marca en la que se ofertan determinados bienes o servicios. El principal problema que plantean es (independientemente del carácter ilícito o no del mensaje publicitario en cuanto pueda resultar engañoso, desleal, etc.) si intrusismo, que en ocasiones puede dificultar el acceso a lo que se busca o se desea ver. Este problema que realmente puede resultar molesto al consumidor o usuario que realice comercio por Internet suele solucionarse mediante programas de ordenador específicos que reconocen este tipo de publicidad e impiden que se descarguen y bloqueen el acceso[53].

El keyword banner es un tipo especial de banner o pop up con un carácter personalizado. La página web que sirve de soporte al anuncio incluye un programa de búsqueda, de tal modo que dependerá de la búsqueda realizada la aparición de un keyword banner u otro. En este supuesto nos encontramos con un tipo de publicidad personalizada que no tiene por qué resultar ilícita por generar confusión en los usuarios a través de la utilización fraudulenta de metatags[54].

Hay "spyware"  que pueden inhabilitar el ordenador y luego anunciar software para solucionar el problema, otros permiten a través de virus por correo electrónico, obtener el número de cuenta bancaria del usuario y otra información importante. También hay casos en que controla el tráfico de Internet, siguiendo la pista de los usuarios sin que los mismos sean concientes y puede resultar difícil de eliminar.

El estado de Utah ha aprobado ya una ley que prohíbe el "spyware". WhenU, al que se impedirá proporcionar anuncios 'pop-up' a los habitantes de Utah, ha recurrido esta ley. Otras compañías dicen que esta norma es demasiado amplia y podía declarar ilegal sin darse cuenta actividades legítimas como apoyo técnico y filtración de contenido[55].

---

[52] www.noticiasdot.com Página visitada el 19 de abril de 2004.

[53] LOPEZ GARCIA, Mabel (2004). “La publicidad y el derecho a la información en el comercio electrónico”. Editado por eumed.net, accesible a texto completo en html://www.eumed.net/cursecon/librería/

[54] DE MIGUEL ASENCIO, Pedro Alberto. “Derecho privado de Internet”. Editorial Civitas. Tercera edición actualizada. Madrid, 2002. Página 160.

[55] www.noticiasdot.com Página visitada el 19 de abril de 2004.

En febrero de 2005 se difundió la noticia que WhenU ganó su segunda batalla judicial respecto al tema "spywares legales"[56]:

“Una juez estadounidense se negó a bloquear a un proveedor de anuncios 'online' en la modalidad 'pop-up', diciendo que era improbable que pudieran confundir a los usuarios de Internet que buscan préstamos para viviendas u otros servicios financieros, informa Reuters. La decisión de la juez de distrito estadounidense Nancy Edmunds es la segunda victoria legal para la firma de anuncios en Internet WhenU, que ha sido demandada por algunos comerciantes 'online' que no quieren que los visitantes de sus propias páginas web vean anuncios 'pop-up' de sus rivales. Wells Fargo & Co. y Quicken Loans demandaron a WhenU, argumentando que la compañía no debería estar autorizada para enviar anuncios a sus visitantes en la web porque esos 'pop-ups' dificultaban la visión de sus sitios y violaban su marca registrada. Pero Edmunds dijo que las compañías no habían demostrado que resultaran perjudicadas por los anuncios de WhenU, que son generados por medio de un 'software' instalado en el ordenador que se instala en este cuando un usuario descarga algunos programas shareware o de libre distribución. Acusado de "spyware" por expertos y sitios especializados, la herramienta usada por WhenU monitoriza la actividad del usuario y muestra "mensajes personalizados" en relación al sitio que se esta visitando o de acuerdo con las preferencias de este. Los usuarios deberían ser capaces de diferenciar fácilmente entre el sitio web que pretenden visitar y los anuncios de WhenU que aparecen en otras ventanas o por debajo del sitio principal, según la opinión de la juez. Otra demanda legal contra WhenU, de la firma de alquiler de camiones U-Haul, unidad de Amerco, fue desestimada en septiembre. La resolución judicial muestra la dificultad de anunciantes y usuarios de protegerse de empresas que de "manera legal" actúan violentando la privacidad del usuario y sus hábitos online”.

Tenemos que tener en cuenta que en estos casos el usuario autoriza la inclusión de estos software al descargar herramientas como Kazaa, eDonkey, entre otras.

Pero en la mayoría de las oportunidades, el spyware se incluye en paquetes de instalación, los usuarios instalan el "paquete al completo" desconociendo que están incorporando un intruso en su computador que vigilará sus actividades y que, además, se dedicará a mostrar anuncios publicitarios en su pantalla.

La barra de Google es Spyware[57]: “La barra de herramientas que Google proporciona gratis, también registra cada página por la que navegas. La política

[56] http://www.noticiasdot.com/publicaciones/2005/0205/0202/noticias020205/noticias020205-09.htm Página visitada el 2 de febrero de 2005.

[57] www.noticiasdot.com “La cara oculta de Google: Afirman que viola la privacidad de los usuarios y vigila sus actividades online”. Página visitada el 30 de abril de 2004.

de privacidad de la Toolbar de Google así lo afirma, pero sólo y exclusivamente porque había un precedente. Alexa perdió un juicio, cuando su barra de tareas hacía lo mismo, pero en la política de privacidad no constaba ni se explicaba".

Earthlink, proveedor de servicios de Internet, ha escaneado 1,06 millones de sistemas durante el primer trimestre de año, concluyendo que cada PC tiene, en promedio, 28 programas espía o spyware[58].

Otro caso es de un malware diseñado para el espionaje industrial[59]: "Detenidos en Israel 18 personas, entre las cuales destacan altos ejecutivos de tres grandes corporaciones, por espionaje industrial a través de troyanos. Durante la investigación se ha localizado, en posesión de los acusados, documentos e imágenes de la competencia y terceras empresas de un enorme valor comercial. Estiman que el espionaje se llevó a cabo durante más de un año. Dejando a un lado los detalles concretos del caso, el problema es que no nos encontramos ante un caso aislado. El hecho de que este tipo de espionaje a través de malware profesional no salga más a la luz se debe en gran parte al sigilo y éxito con el que se llevan a cabo los ataques, no a la ausencia de ellos. Una imagen vale más que mil palabras: desde documentos confidenciales, hasta la foto de la hija que un directivo tiene como fondo de escritorio, pasando por un vídeo que muestre todo lo que visualizó su pantalla durante varias horas la jornada anterior".

## 2.4 Adware

El adware es la versión "legal" del spyware. Son pocas las diferencias existentes entre uno y otro. El adware se instala en nuestro ordenador de "manera legal", mientras que el segundo llegó a nuestro equipo camuflado en un virus o visitando una página web cuyo propietario carece totalmente de escrúpulos. Ambos, sin embargo, actúan de la misma manera, monitorizando la actividad del usuario y violando su privacidad.

El adware es uno de los malware (amenazas) más difundidos en Internet, el que en términos simples consiste en una aplicación diseñada para mostrar al usuario publicidad no solicitada. Todos hemos sido víctimas, más de una vez, de los ataques o más bien de la lluvia de publicidad que inunda el correo electrónico, sin que sepamos cómo dieron con nuestra dirección o cómo notaron qué productos nos gustaban[60].

---

[58] http://www.noticiasdot.com/publicaciones/2004/0404/2104/noticias210404/noticias210404-7.htm

[59] http://www.hispasec.com/unaaldia/2410 Página visitada el 13 de junio de 2005

[60] http://www.noticiasdot.com/publicaciones/2005/0205/0902/noticias090105/noticias090205-15.htm Página visitada el 9 de febrero de 2005.

Pero el adware es una clase de licencia de software, la cual se acepta para utilizar determinados programas. Dicha licencia ofrece el uso de una aplicación con el único costo de visualizar una serie de mensajes publicitarios.

Sin embargo, hay oportunidades en que estos programas reúnen información acerca de los hábitos de navegación del usuario, las páginas visitadas o el inventario de las aplicaciones instaladas en el equipo, con el fin de enviar y vender dichos datos a empresas de publicidad en Internet.

En otras ocasiones, muchos adware se instalan de forma “simulada”, ya que piden permiso al usuario pero mostrándole mensajes intercalados en las pantallas de instalación de otros programas. De esta forma, la persona da su “consentimiento” para la instalación del adware, sin fijarse realmente en lo que está haciendo.

Una vez que un adware se instaló en un sistema, se conecta a un servidor que le indica los anuncios que tiene que mostrar. Para ello, mientras el usuario se encuentra navegando por Internet, el adware abre una conexión con la máquina remota para, acto seguido, abrir una ventana publicitaria ante los ojos del usuario. En muchas ocasiones, éste no sabe si el pop-up corresponde a la página que está visitando, o si tiene algún adware instalado en el sistema. De por sí, este proceso ya es perjudicial para el usuario, ya que estas consultas al servidor bajan la velocidad de la conexión a Internet[61].

## 2.5 Phishing

Los ataques de estafa a través de Internet por el método de "phishing", que significa "pesca" en el argot informático, se han ido incrementando.

El sistema más utilizado por los cyber-estafadores es el envío de correos electrónicos con falsos remitentes, como por ejemplo de entidades financieras, de forma tal que las víctimas cliquearan en un link y de esa forma podían obtener información personal.

Pero ya se habla de una nueva generación de phishing. Hispasec[62] demuestra cómo es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la parte inferior del navegador certifique que se encuentra en el servidor seguro del banco.

[61] http://www.noticiasdot.com/publicaciones/2005/0205/0902/noticias090105/noticias090205-15.htm Página visitada el 9 de febrero de 2005.
[62] http://www.hispasec.com/unaaldia/2406 Página visitada el 13 de junio de 2005.

Hasta el momento las recomendaciones que se hacían para acceder de forma segura a la banca electrónica eran: comprobar que la URL del navegador comenzara por https:// seguido del nombre de la entidad y comprobar el certificado de que se había ingresado en un servidor seguro, haciendo doble click en el candado que aparece en la parte inferior del navegador. Esto hoy día ya no es tan seguro.

## 2.6 Derivados del Phishing[63]

### 2.6.1 Scam

A este tipo de fraude también se lo conoce como phishing laboral, porque tiene como objetivo obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias.

Las modalidades utilizadas consisten en envíos masivos de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.

### 2.6.2 Smishing

Esta es otra variante del phishing, pero el ataque se realiza a través de los mensajes a teléfonos móviles. El resto del procedimiento es igual al del phishing, el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falsa, idéntica a la de la entidad en cuestión.

### 2.6.3 Spear Phishing

También estamos, en este caso, ante un sub tipo de phishing en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional.

### 2.6.4 Vishing

Esta clase de fraude también persigue la obtención de datos confidenciales de los usuarios, pero a través de la telefonía IP. Los ataques de vishing se suelen producir siguiendo dos esquemas[64]:

[63] VIEGA, María José. “Delitos informáticos: manipulación de la información pública y privada”. II Jornadas Rioplatense de Derecho Informático. Buenos Aires, 18 de agosto de 2011.

- Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita.

- Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etc.

## 2.7 Pharming

El pharming deriva del término *farm,* granja en inglés, expresión que es utilizada cuando el atacante ha conseguido acceso a un servidor DNS o varios servidores, en este último caso granja de servidores o DNS.

Esta modalidad de fraude online ataca la vulnerabilidad del software de los servidores DNS o de los equipos de los propios usuarios, redireccionando el nombre de dominio a un sitio web falso, diseñado por el atacante. Es utilizada para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos personales del usuario, generalmente datos bancarios.

Si el phishing engaña a los usuarios uno por uno, conduciéndolos a visitar un sitio apócrifo de su banco o comercio preferido, el pharming interviene las comunicaciones entre el usuario y su proveedor de Internet (ya sea un proveedor de comunicaciones, o un servidor corporativo) para lograr que cuando un usuario teclea en su navegador una dirección legítima, éste sea conducido a una falsificación de la página Web que quiere visitar y sea ahí donde introduzca los datos de su cuenta[65].

Por tanto, el riesgo para el usuario en los casos de pharming es diferente, mientras que en el phishing requiere una actitud activa, hacer click en el link del correo electrónico, en el pharming el fraude se produce sin participación directa del usuario. La utilización de medidas técnicas de seguridad en un sistema,

---

[64] http://www.delitosinformaticos.info/delitos_informaticos/glosario.html Página visitada 21 de junio de 2010.

[65] http://www.mx.terra.com/tecnologia/interna/0,,OI889426-EI4906,00.html Página visitada 21 de junio de 2010. El Pharming: amenaza de fraude a negocios. Trend Micro. 21 de febrero de 2006.

como por ejemplo un firewall, herramientas de protección contra adware y spyware, contrarrestan este tipo de amenazas[66].

El pharming se realiza modificando el software, lo cual puede realizarse en forma remota o introduciendo un programa que lo realice en forma automática. Para ello es necesario introducir un troyano en el disco duro de la víctima, el cual puede autoeliminarse, borrando del disco duro las huellas del ataque.

### 2.8 Scavenging

Es la apropiación de informaciones residuales, la que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

## 3. PUBLICIDAD

Partamos del concepto que la publicidad en la red no consiste únicamente en anunciar y distribuir mensajes. También facilita las relaciones con los clientes, la creación de *ciber-marcas*, proporciona servicios al consumidor, genera ventas electrónicas de artículos y servicios, envía eficientemente mensajes de marketing a la audiencia adecuada y logra crear una personalización de servicios para grandes masas de consumidores así como un marketing directo e interactivo[67].

Por esto motivo, tanto el marketing como la publicidad se tratan de actividades vinculadas a empresas y todo tipo de entidades que se realiza a través de diferentes canales, como por ejemplo el correo postal, el correo electrónico, el teléfono, los mensajes al teléfono celular.

“Al acometer un tema sobre protección de datos y publicidad ha de recordarse que toda publicidad se crea para ser comunicada, para ser difundida y tal difusión puede realizarse a través de distintos canales de marketing, como televisión, radio, correo postal, internet, etc. La publicidad puede afectar a distintos bienes jurídicos, por ello los distintos ordenamientos jurídicos regulan

[66] VIEGA, María José y CARNIKIAN, Federico. “Respuesta a los delitos informáticos: su visión desde la privacidad y la seguridad de la información”. Ponencia presentada al Seminario Nuevas Tecnologías: Privacidad y Seguridad. Cartagena de Indias, 21 al 23 de julio de 2010.
[67] MEEKER, Mary. “La publicidad en Internet”. Ob. Cit.

la forma de llevarla a cabo así como sus contenidos, sobre todo con la finalidad de tutelar los derechos de los consumidores y usuarios"[68].

Según el Diccionario de la Real Academia Española se entiende por publicidad la divulgación de noticias o anuncios de carácter comercial para atraer a posibles compradores, espectadores, usuarios, etc.

Para Jesús Rubí es aquella comunicación que tiene como finalidad la comercialización de los productos o servicios de una empresa, es decir la que va dirigida a promover la contratación, como por ejemplo la realizada con fines de venta directa. (…) Quedarían incluidos en el campo de las comunicaciones comerciales los tratamientos que se realizan con fines de prospección comercial, como los estudios de mercado que se realizan antes de lanzar un determinado producto al mercado, si para ello se emplearon datos de carácter personal[69].

Las ofertas promocionales como descuentos, premios y regalos, concursos o juegos promocionales quedan incluidas en el concepto de publicidad porque el fin que se persigue es promover la venta del producto o servicio que se promociona, de acuerdo a lo que establece la Directiva 2000/31/CE.

En España, la Agencia Española de Protección de Datos analiza este tema en el procedimiento Nº PS/00183/2009. "En este caso se consideró que eran comunicaciones comerciales los correos electrónicos que promocionaban la participación en un concurso, en el que se obtendría el premio consistente en dos entradas VIP para asistir al concierto de una popular cantante que se celebraría en España, ya que la finalidad del concurso era la de incentivar los productos y servicios prestados por la empresa que organizaba el concurso".

Pero nos encontramos con comunicaciones excluidas del concepto de comunicación comercial, ellas son:

a) Las comunicaciones **meramente informativas**, muchas veces es en cumplimiento del deber de informar que atañe a los fabricantes, empresarios y comerciantes. Ej.: los movimientos de una cuenta bancarias, condiciones de un servicio contratado, etc.

b) Las comunicaciones **con contenido político o sindical**, como por ejemplo la propaganda sindical o electoral. Pero hay que tener en cuenta que las comunicaciones enviadas por este tipo de agrupaciones pero con finalidad

[68] RUBI NAVARRETE, Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Tratamientos específicos (I). Marketing. Telecomunicaciones. Solvencia patrimonial. Tratamiento de Datos en el ámbito de la salud.
[69] RUBI NAVARRETE, Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Ob. Cit.

comercial, la comunicación será considerada comercial, como el caso en que se pretende captar fondos.

La Agencia Española de Protección de Datos, en el Procedimiento PS/00147/2008. “En este caso un partido político remitió, a través del correo electrónico, mensajes en los que se promocionaba la contratación de una hipoteca. El correo contenía información acerca de un sistema de hipoteca que la organización política ponía a disposición de las familias españolas y cuya gestión se realizaría por varias redes inmobiliarias, además del citado correo contenía dos links a direcciones electrónicas en las que se ofrecía más información. Se consideró que, en este caso, el contenido del mensaje quedaba incardinado en el concepto de comunicación comercial, al promover la contratación de unas hipotecas, aunque hubiera sido remitido por un partido político”.

En Uruguay, la Unidad Reguladora y de Control de Datos Personales (URCDP) en el Dictamen N°4/2009 de 22 de mayo de 2009 analiza la consulta sobre la publicidad que realizan los partidos políticos y establece en el considerando IV que: “en todo caso existe siempre la posibilidad de apelar al procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables (arts. 4 literal G, 17 literal D). Se menciona como ejemplo, la existencia de programas informáticos que permiten realizar llamados telefónicos en forma aleatoria, generando el número en forma randómica, lo que no constituye una base de datos”. Y dictamina: “I) En lo que respecta a la competencia de esta Unidad, cuando la difusión se realiza -en el caso de personas físicas- utilizando fuentes públicas de información como la Guía Telefónica, o bien se trata de números pertenecientes a personas jurídicas, dicha difusión resulta legítima. II) En cualquier caso se considera lícita la posibilidad de disociación de la información de forma tal de volverla anónima, lo que puede hacerse mediante la utilización de listados que las empresas telefónicas cabe que suministren a terceros conteniendo exclusivamente números de teléfono, sin agregados ni conexiones con ninguna otra clase de datos que llevase a determinar los titulares de tales servicios. Sobre el punto, téngase presente, además, lo informado en el Considerando IV”[70].

c) La legislación española no considera comunicación comercial a **los mensajes que contengan únicamente un nombre de dominio** (o dirección electrónica) o una dirección de correo electrónico cuando sean elaboradas por un tercero y sin contraprestación económica.

La Agencia Española de Protección de Datos no considera comunicación comercial el mensaje de correo electrónico que, sin ningún tipo de información

[70] UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES. Libro de Resoluciones, dictámenes e informes. Año 2009.

comercial, contiene un link a la página web de una empresa. Sin embargo, no deja por ello de constituir spam al no ser un mensaje solicitado.

Según MANZANARES GALEAN: “El marketing es considerado como uno de los sectores con mayor índice de riesgo de cara a incurrir en las infracciones tipificadas en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal”[71].

[71] MANZANARES GALEAN, Llanos y otro. “Implicaciones de la protección de datos en el marketing”, en MK Marketing+Ventas N° 199, Febrero de 2005. Página 22. http://pdfs.wke.es/8/7/8/6/pd0000018786.pdf

# CAPITULO III

# MARCO NORMATIVO

## 1. UNION EUROPEA

En los años 70 se constata en Europa la importancia del uso de las telecomunicaciones y por tanto la necesidad de una legislación uniforme y que proteja los derechos y libertades fundamentales. El Convenio 108 de 28 de enero de 1981 del Consejo de Europa estable una serie de principios básicos para la protección de datos y criterios para el flujo de ellos, creando un Comité Consultivo.

Se realiza una enumeración de los principios de la protección de datos:

*Principio finalista*: debe establecerse la finalidad que tiene el banco de datos, debiendo ser constatable en todo momento la pertinencia de los datos, el principio de utilización no abusiva y el principio del derecho de olvido.

*Principio de lealtad*: la recopilación de datos debe realizarse por medios lícitos.

*Principio de exactitud*: el responsable del banco de datos debe comprobar la exactitud de los datos y mantenerlos actualizados.

*Principio de publicidad*: debe existir un registro público de los ficheros.

*Principio de acceso individual*: toda persona tiene derecho a acceder a sus datos automatizados y a obtener copia de ellos.

*Principio de seguridad*: las bases de datos deben estar protegidas.

El artículo 6 del Convenio refiere a los hoy llamados datos sensibles y como deben ser tratados. También se expresa el compromiso de las partes contratantes de establecer un régimen de recursos y sanciones que garanticen el cumplimiento de los principios.

No quiero dejar de destacar que Uruguay está en proceso de ratificar el Convenio 108 y su Protocolo Adicional, habiendo sido invitado por el Consejo de Europa por lo que se está llevando a cabo el procedimiento normativo interno a tales efectos, encontrándose en este momento el proyecto de ley a estudio del Parlamento Nacional. Esto ratifica la voluntad del país de proteger el derecho fundamental a la protección de datos personales.

El 14 de junio de 1985 se suscribió el Acuerdo de Schiengen, que es un elemento de coordinación interestatal, que afecta el tratamiento y la protección de datos, aunque no sea concreto de este tema como el Convenio 108 o la Directiva 95/46/CE, interesa destacar que el acuerdo regula el flujo transfronterizo de datos de carácter personal.

### 1.1. Directiva 95/46/CE de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

La Directiva establece como eje central de su contenido el derecho a la intimidad, sin que excluya otros derechos fundamentales. El artículo 2 da una serie de definiciones que son coincidentes con las establecidas en el Convenio 108[72].

El ámbito de aplicación se encuentra regulado en su artículo 3, aplicándose tanto a los tratamientos automatizados de datos como a los manuales. Se excluye:

a. El tratamiento realizado por una persona física en el ámbito exclusivamente personal o doméstico.

b. Cuando el tratamiento tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.

En el Considerando 24 se establece que están bajo la protección de la Directiva todos los datos que tradicionalmente se han venido considerando datos personales, lo cual debe interpretarse como una remisión al Convenio 108. Y parece interesante destacar el Considerando 14 en el que se establece que la Directiva se aplicará a datos de sonido e imagen.

Regula, también, las comunicaciones comerciales cuando se utilizan datos de carácter personal, independientemente del canal que se utilice y faculta a los Estados miembros a establecer condiciones y requisitos para la comunicación de datos personas a terceros con fines de prospección comercial (Considerando N° 30) y declara expresamente que no se opone a que se regulen las actividades de este tenor, referidas a consumidores que residan en el territorio del Estado miembro que así lo disponga, siempre que ello no afecte la protección de las personas en lo que respecta a tratamientos de datos (Considerando N° 70).

[72] REBOLLO DELGADO, L y SERRANO PEREZ, M: “Introducción a la protección de datos”. 2ª Edición. Madrid, 2008.

También, en el artículo 14 b de la Directiva se ordena a los Estados miembros que reconozcan a los interesados el derecho de oposición al tratamiento de datos de carácter personal, cuando el responsable realice o prevea un tratamiento destinado a la prospección.

Es de destacar que Uruguay ha solicitado la adecuación a esta Directiva, habiéndose expedido el Grupo de Trabajo del Artículo 29 en forma favorable mediante el Dictamen N° 6/2010 de 12 de octubre de 2010.

### 1.2 Directiva 2000/31/CE de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior

Al analizar la Directiva 2000/31/CE, llamada de Comercio Electrónico relativo al régimen de las comunicaciones comerciales Delpiazzo y Viega decían que[73]:

a. Debe identificarse claramente: que se trata de comunicación comercial y la persona física o jurídica en nombre de la cual se realizan las comunicaciones.

b. Listas de exclusión voluntarias (opt-out): para inscribirse las personas que no deseen recibir comunicaciones comerciales (Directiva 97/7/CE). La directiva objeto de estudio prevé que quienes realicen comunicaciones no solicitadas consulten las listas de exclusión y las respeten.

Pese a que en un principio la Directiva 2000/31/CE estableció la necesidad de que los Estados miembros que hubieren permitido el envío de comunicaciones comerciales no solicitadas garantizasen la consulta de las listas de exclusión voluntaria (opt out) y las respetasen, sin embargo, esta situación ha cambiado con la aprobación de la Directiva 2002/58/CE, en la que se ha previsto el sistema contrario (opt in) como regla general[74].

Las legislaciones, a fin de procurar la defensa de los consumidores y usuarios y de proteger los datos personales de los destinatarios de la publicidad, arbitran reglas para regular las comunicaciones comerciales. En general, las soluciones adoptadas se pueden reconducir a dos:

- Sistema de opt in (registro de inclusión o también denominado listas blancas): se trata de un sistema que requiere el consentimiento del destinatario para que el envío de la comunicación se considere lícito. El

[73] DELPIAZZO, Carlos y VIEGA, María José. "Lecciones de Derecho Telemático". Tomo I. Fundación de Cultura Universitaria. Lección 8 página 115. Montevideo, abril de 2004.
[74] VAZQUEZ RUANO Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Página 334.

sistema comunitario europeo admite el sistema opt in debido a que el consentimiento previo es el principio en materia de comunicaciones comerciales, aunque existen excepciones al principio del previo consentimiento. En España, también se opta por el sistema opt in y se prohíbe el envío de comunicaciones comerciales que no hayan sido autorizadas en forma previa[75].

- Sistema opt out (registro de exclusión o listas negras): este sistema no exige que el destinatario de la comunicación preste su consentimiento previo, pero prohíbe el envío de dichas comunicaciones a las personas que hayan manifestado su deseo de no recibir publicidad, como por ejemplo en Estados Unidos.

Estas listas pueden ser públicas (nacionales o internacionales) o privadas. Las primeras, deberán ser consultadas de forma periódica por los anunciantes y en un momento previo al de la remisión de las comunicaciones comerciales que no se hubieren solicitado. Las segundas, por su parte, pertenecen a un determinado empresario. El cual se abstendrá de enviar mensajes publicitarios a aquellos sujetos que han manifestado su oposición a la recepción de los mismos[76].

A través de los "Ficheros Robinson" se ofrece a los interesados la posibilidad de inscribirse con la finalidad de no recibir más publicidad. Dentro de este tipo de ficheros, pueden diferenciarse dos modalidades[77]:

- Los "ficheros Robinson" que gestiona cada responsable, que obtuvo inicialmente los datos personales para el envío de publicidad, en los que se incluyen los datos de las personas que han manifestado su oposición o negativa a recibir publicidad de ese responsable, ya se trate de publicidad de sus productos, de terceras empresas o de publicidad emitida en el marco de campañas publicitarias contratadas con terceros.

- Los ficheros comunes de exclusión, cuya finalidad es evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

Por tanto, consisten en ficheros elaborados a raíz del ejercicio de oposición y tienen el efecto de neutralizar los datos contenidos en los ficheros de datos. Así, tras la oposición de su titular, la empresa que elabora una de estas listas no procede a la cancelación de sus datos sino a incorporarlos a otro fichero cuya

[75] RUBI NAVARRETE, Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Ob. Cit. Página 9.
[76] VAZQUEZ RUANO Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Páginas 335 y 336.
[77] RUBI NAVARRETE, Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Ob. Cit. Página 25.

función es negativa, pues borrarán los datos de otros ficheros cuando éstos se crucen con aquéllos. Como pueden comprobarse, cumplen también una función de organización y complementaria a la gestión de los ficheros de carácter personal. No obstante, cierto sector de la Doctrina ha puesto de manifiesto que esta práctica "a veces no surte el efecto deseado, dado que los registros utilizados como listas Robinson y las bases de datos sobre las que se cruzan los datos, no coinciden en tipo y características de las letras, al existir acentos y letras distintas, sin quedar eliminados los registros que se cruzan al no coincidir los caracteres de éstos, aunque se refieran y correspondan a la misma persona física identificada o identificable" (AA.VV.: la protección de datos en la gestión …, pgs. 145 y 146)[78].

Los sistemas opt in y opt out tienen, cada uno de ellos, sus ventajas e inconvenientes y difieren en razón de la consideración del usuario receptor de las comunicaciones comerciales o de las empresas anunciantes que las remiten.

Respecto a las listas opt in, en principio desde la óptica del usuario, la necesidad de que éste otorgue su expreso consentimiento proporciona un mayor nivel de seguridad y confianza en la Red. Pues ello implica que de forma previa ha debido ser informado explícitamente de todos los extremos. Además, y como consecuencia de ello, disminuyen los riesgos y costes adicionales provocados por la recepción de comunicaciones comerciales de forma masiva. Y en lo que concierne a la entidad anunciante, el envío de la promoción sólo a los sujetos que hubieran manifestado su deseo de recibirla, beneficia a la imagen de la entidad. Lo que, en último término, puede reflejarse en la contratación del bien o en la adquisición de numerosas reclamaciones de los sujetos no interesados en la publicidad. Ha de tenerse en cuenta que el establecimiento de este servicio implica la posibilidad de utilizar el sello correspondiente en la acciones que se lleven a cabo en el marco comercial. Y ello va a ser una entidad anunciante[79].

Por otra parte, el sistema opt out tiene el inconveniente para el consumidor que recibirá comunicaciones comerciales hasta el momento en el que manifieste su rechazo. Para algunos autores esto es razonable y no puede considerarse una carga desproporcionada para los usuarios. Sin embargo, muchas veces los usuarios no toman la iniciativa de inscribirse, a veces por desconocimiento de las propias listas. También debe tenerse en cuenta, que los mensajes se envían a un correo privado del consumidor, lo que puede implicar una violación a su privacidad. Pero, obviamente, es un sistema ventajoso para las empresas ya

[78] DE LA VEGA GARCIA, Fernando L. "Datos personales y deberes del empresario en la publicidad". Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009. Página 32.

[79] VAZQUEZ RUANO Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Página 336.

que reducirán sus inversiones publicitarias e implica el ejercicio de la libertad de empresa y de información comercial.

### 1.3 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

La Directiva 2002/58/CE sobre la Protección de Datos sobre tráfico de telecomunicaciones está prevista en esta Directiva del Parlamento Europeo y del Consejo, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas (Diario Oficial L 201/37), en virtud de la cual el tratamiento de datos de tráfico está permitido, en principio, para facturación y para pagos de interconexión. Tras debates prolongados y explícitos, la retención de datos de tráfico con vistas a la aplicación de ley debería respetar estrictas condiciones de conformidad con el apartado 1 del artículo 15 de la Directiva: es decir, en cada caso sólo por un período limitado y cuando constituye una medida necesaria proporcionada y apropiada en una sociedad democrática[80].

La Directiva exige, además de consentimiento previo, para comunicaciones no solicitadas o spam una dirección de respuesta válida donde la persona pueda solicitar que no le envíen más mensajes. Por otra parte, es ilícito disimular u ocultar el remitente.

De acuerdo con la Directiva sería posible manifestar el consentimiento mediante la selección de una casilla de un sitio web en Internet. La doctrina viene admitiendo, igualmente, la posibilidad de que se preste el consentimiento expreso por medios electrónicos. Así se ha entendido que podría prestarse, entre otros medios, mediante la remisión de un correo electrónico aceptando el envío de la comunicación comercial, mediante un texto declarativo de la voluntad cumplimentado por el interesado e inserto en la página web del anunciante, o bien pulsando un icono, botón, tecla o pulsador habilitado a tal efecto en el sitio web[81].

El supuesto excepcional previsto en la Directiva respecto al envío publicitario a sujetos con los que previamente se hubiere mantenido una relación contractual y los datos de contacto se recabasen de forma lícita se aproxima, al igual que en la Can Spam Act 2003, al sistema opt out. Esto es, se permite la remisión de comunicaciones electrónicas comerciales hasta el momento en el que el

[80] Dictamen 5/2002 aprobado el 11 de octubre de 2002, sobre la Declaración de los Comisarios responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de setiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones.

[81] RUBI NAVARRETE, Jesús. Curso CEDDET: “El Derecho a la protección de datos personales, 1ª edición”. Módulo 4. Ob. Cit. Página 16.

destinatario de las mismas manifieste su voluntad negativa a dicha recepción, mediante su inscripción en una lista. Exigiéndose que dichas comunicaciones estén debidamente identificadas[82].

Como manifiesta Trinidad Vázquez la Directiva sólo acoge el sistema opt out para aquellos casos en que el correo electrónico se entregó en el marco de una relación contractual. Pero para que pueda llevarse a cabo se requieren los siguientes elementos:

1. La dirección de correo electrónico debe obtenerse en forma lícita.

2. Los productos que se ofrezcan deben ser de la empresa con la cual se contrató.

3. Debe tratarse de productos similares a los contratados por el cliente.

4. Al momento de recabar el dato debe darse al cliente información sobre el uso de la misma, advertir que podrá utilizarse para venta directa y dar al cliente la posibilidad de que se oponga.

La Directiva prevé la necesidad de informar de manera clara y concisa al interesado sobre el establecimiento de las cookies en su terminal informático. El legislador comunitario en el cumplimiento de dicho deber se remite expresamente a los presupuestos indicados en la Directiva 95/46/CE.

Merece especial atención cuestionarnos sobre la información que se ha de facilitar al usuario en cuanto a los datos que se pretenden almacenar en el archivo cookie; el lugar en el que permanecerá la información recabada; la finalidad que justifica el establecimiento del archivo y el plazo de tiempo de vigencia del mismo[83].

La Directiva responde al primer interrogante determinando que se ponga en conocimiento del usuario la pretensión de instalar la cookie en forma previa a la instalación, lo cual no genera dudas.

El problema que se plantea es la posibilidad de que la información facilitada al momento de la conexión abarque cualquier conexión futura y analizando la posibilidad de negativa por parte del usuario a que la instalación se realice.

Tanto la información relativa a la utilización de estos dispositivos de obtención de datos en la Red que se vayan a establecer en el ordenador del usuario,

[82] VAZQUEZ RUANO Trinidad. “La protección de los destinatarios de las comunicaciones comerciales electrónicas”. Ob. Cit. Página 335.

[83] VAZQUEZ RUANO, Trinidad. “La protección de los destinatarios de las comunicaciones comerciales electrónicas”. Ob. Cit. Página 168.

como la facultad de éste de impedir su instalación podrá efectuarse en una misma conexión, pero referirse también a otras conexiones que se realicen a posteriori desde ese mismo equipo informático. Lo cual entendemos que va a suponer un perjuicio para los usuarios, en tanto que no siempre el uso de un determinado terminal informático se realiza por la misma persona y ello trae como consecuencia que si el primer sujeto que utiliza el ordenador para conectarse a Internet acepta el uso de archivos cookies, los usuarios que después se conecten a la Red desde ese mismo ordenador tendrán que soportarlos, aún sin tener conocimiento de que sus datos e información está siendo recabada. Por lo que, en nuestra opinión, debiera haberse limitado más esta posibilidad a fin de tutelar correctamente la intimidad y garantizar la protección de la información personal de los usuarios en un entorno como el electrónico[84].

Téngase presente que las cookies recuerdan los usuarios y contraseñas, lo que implica un peligro para el usuario inicial, el uso que los usuarios posteriores hagan de esa información. Por otra parte, la Directiva 95/46/CE se ocupa solamente de la responsabilidad del sujeto que trata los datos personales y su obligación de cancelarlos una vez que se ha cumplido con la finalidad de la recolección.

El responsable de la instalación de las cookies debe informar el plazo de duración ya que las cookies pueden ser de carácter temporal o permanente, siendo estas últimas más peligrosas para vulnerar la privacidad.

Por otra parte, expresa la Directiva que tanto la información como la posibilidad de oponerse a la instalación de las cookies "*debe ser tan asequible para el usuario como sea posible*". Sin lugar a dudas la información deberá ser clara y precisa, entendiendo que el idioma deberá ser aquel con que está configurado el navegador.

Respecto a este punto Trinidad Vázquez entiende que "puede pensarse que será aquel utilizado por el navegador del usuario, ya que la información debe hacerse efectiva respecto del mismo a efectos de que éste reciba una adecuada protección de sus intereses y derechos, se debiera optar por informarle en la lengua que por defecto emplea en su navegador. Si nos mostramos partidarios con esta primera opción, los servidores que insertan archivos cookies o similares en el ordenador que accede a una determinada página de Internet y que tiene la obligación de informar al usuario afectado por los mismos, habrá de modificar su comunicación electrónica informativa en razón del idioma empleado por el navegador que, en cada caso, le solicita la página desde la que dichos archivos se establecen. Lo cual entendemos, puede traducirse en un esfuerzo excesivo si se tiene en cuenta, además, que el deber

[84] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Página 168.

de información previo al que hacemos referencia solo puede eludirse en las ocasiones expresamente indicadas en la norma"[85].

Las Recomendaciones de la Agencia de Protección de Datos establece que el idioma que se emplee en cuanto al cumplimiento de la obligación de informar al interesado respecto del tratamiento de los datos que le pertenecen será el mismo que se utilice a posteriori para recabar dichos datos y tratarlos en los términos de la norma[86].

Desde el punto de vista económico se ha manifestado que este requerimiento implica un costo muy importante debido al rediseño de todos los sitios web y por otra parte, la desventaja para los países europeos frente a otros países que no tienen estas exigencias.

Desde un punto de vista jurídico el problema que plantea la Directiva refiere a la obtención del consentimiento, ya que remite a la Directiva 95/46/CE que establece que el consentimiento debe ser libre, específico e informado. Por tanto, éstas deberán ser las características del consentimiento a los efectos de la instalación de las cookies.

Las opciones que el usuario tiene para manifestar su voluntad a través del navegador son:

a. La aceptación general de las cookies.

b. El rechazo de la instalación de las cookies o la consulta cada vez que el usuario ingresa al sitio web.

Desde un punto de vista práctico, podrían implementarse:

i. Una ventana electrónica donde el usuario pueda aceptar la instalación de las cookies.

ii. Una cláusula contractual cuando se trate de un contrato on line, la que no podrá ser obligatoria, ya que podría considerarse abusiva.

Un supuesto diferente sería que el usuario tenga configurado el navegador de forma tal que acepta la instalación de cualquier cookie, ¿estamos ante un caso de consentimiento implícito o tácito?

Trinidad Vázquez admite el consentimiento implícito o tácito en este caso. Puesto que, lo que a la luz de la norma comunitaria interesa respecto de la

[85] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Páginas 171 y 172.
[86] (AEPD año 2002 1° Recomendación.

manifestación de su voluntad es el conocimiento y la información previa que el usuario afectado hubiere recibido. Y si éste, teniendo conocimiento de que la configuración del navegador que utiliza admite cookies no manifiesta su oposición, implícitamente otorga su voluntad de aceptarlos[87].

### 1.4 Directiva 2009/136/CE de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE, la Directiva 2002/58/CE y el Reglamento (CE) N° 2006/2004

La Directiva 95/46/CE referente a la protección de las personas físicas relativo al tratamiento de los datos personales y a la libre circulación de éstos, se aplica en los asuntos no cubiertos específicamente por la Directiva modificada.

El artículo 5 apartado 3 exige el consentimiento autorizado del abonado o usuario para almacenar información legalmente u obtener acceso a información almacenada en su equipo terminal.

Se establece en el Considerando 66 de la Directiva que: “Puede que haya terceros que deseen almacenar información sobre el equipo de un usuario o acceder a la información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espías o los virus). Resulta, por tanto, capital que los usuarios reciban una información clara y compleja cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso. El modo en que se facilite la información y se ofrezca el derecho de negativa debe ser el más sencillo posible para el usuario. Las excepciones a la obligación de facilitar información y proponer el derecho de negativa deben limitarse a aquellas situaciones en las que el almacenamiento técnico o el acceso sean estrictamente necesarios con el fin legítimo de permitir el uso de un servicio específico solicitado específicamente por el abonado o usuario. Cuando sea técnicamente posible y eficaz, de conformidad con las disposiciones pertinentes de la Directiva 95/46/CE, el consentimiento del usuario para aceptar el tratamiento de los datos puede facilitarse mediante el uso de los parámetros adecuados del navegador o de otra aplicación. La aplicación de estos requisitos debe ganar en eficacia gracias a las competencias reforzadas concedidas a las autoridades nacionales”.

Por lo tanto, todo almacenamiento de cookies o cualquier otro sistema similar y la utilización posterior de cookies que hayan sido previamente almacenados para tener acceso a información de los usuarios debe cumplir con el artículo 5 apartado 3. Este artículo es neutro tecnológicamente por lo que aplica a

[87] VAZQUEZ RUANO, Trinidad. “La protección de los destinatarios de las comunicaciones comerciales electrónicas”. Ob. Cit. Página 180.

cualquier tecnología utilizada para almacenar o acceder a información almacenada en el equipo de los usuarios.

Por otra parte, no tipifica la información, por lo que no requiere que sean datos personales, sino que posee mayor amplitud, ya que refiere a la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

El Grupo de Trabajo del Artículo 29 en su Dictamen 1/2008 de 4 de abril de 2008 sobre cuestiones relacionadas con motores de búsqueda determina que, en la mayoría de los casos, las cookies y las direcciones IP deben ser considerados datos personales. “Cuando una cookie contiene un identificador único de usuario, éste es claramente un dato personal. La utilización de una cookie permanente o de dispositivos similares con un identificador único de usuario permite seguir a los usuarios de un ordenador concreto, incluso en caso de utilización de direcciones IP dinámicas. Los datos sobre comportamiento generados por la utilización de estos dispositivos permiten centrarse más aún en las características personales del individuo en cuestión”.

## 2. ESPAÑA

En España podemos destacar la siguiente normativa vinculada a la temática:

Ley orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD),

Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico (LSSI).

Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones (LGT), confiere a la Agencia de Protección de Datos competencias para hacer cumplir las disposiciones relativas al envío de comunicaciones comerciales.

La LSSI con relación al envío de mensajes publicitarios electrónicos requiere el consentimiento expreso, por lo que resulta más estricta que la LOPD que requiere el consentimiento inequívoco para la obtención de los datos con finalidad comercial.

Este diferente tratamiento plantea el interrogante acerca de cuál es la norma aplicable, pues en materia de protección de datos e intimidad la LOPD es especial respecto de la LSSI. Por tanto debiera anteponerse a la LSSI.

Sin embargo, en el tema de las comunicaciones comerciales el problema se agrava, ya que en este caso la protección de la intimidad responde a la necesidad de conocer los datos para remitir la publicidad por vía electrónica. En este sentido la doctrina se halla dividida: de un lado, los autores que han considerado que en materia de protección de datos en Internet la LOPD debe adaptarse a la LSSI, por lo que se exigirá el consentimiento expreso no solo para la obtención de los datos, sino también para la posterior remisión publicitaria. Sin embargo, de otro lado se hallan aquellos para los que el rango y la especialidad de la LOPD y la explícita remisión establecida en el propio artículo 19 LSSI hace que esta norma sea la que prevalezca. Por lo que el consentimiento expreso sólo se impondrá respecto del envío promocional. En nuestra opinión, y basándonos en la especialidad de la materia (el envío publicitario electrónico), debiera aplicarse la LSSI y en materia de obtención de los datos personales para dicho envío comercial los presupuestos de la LOPD[88].

Podemos concluir en base a esta opinión que el punto de equilibrio entre los intereses del anunciante y del usuario se va a dar por el acuerdo entre la empresa y el receptor de la publicidad referido al envío comercial, estando ante el sistema opt in porque frente al ofrecimiento publicitario es el usuario quien otorga su consentimiento o no.  A esta técnica se la denomina marketing de permiso o "*permission marketing*".

Sin embargo, la Directiva 2002/58/CE, la LSSI (apartado 2° del artículo 21) y la LOPD (artículo 6) exceptúan la aplicación de esta técnica cuando se ha mantenido una relación contractual previa con el sujeto destinatario del mensaje.

Como hemos visto en los puntos anteriores, en Europa, en general, no es suficiente que exista una relación comercial para que una empresa pueda enviar publicidad a sus clientes, es necesario que tenga su consentimiento para hacerlo, aunque este consentimiento puede recabarse en cualquiera de las formas legalmente admitidas. Cuando entre las partes existe un contrato, debe poseer la opción de que el interesado manifieste si desea recibir comunicaciones o no.

Una Sentencia de la Audiencia Nacional, de 5 de noviembre de 2008 consideró válido el procedimiento utilizado por una empresa para recabar de sus clientes el consentimiento tácito con la finalidad de utilizar los datos de contratación y facturación con fines publicitarios. Dicho procedimiento consistió en la remisión a los clientes de la empresa de un escrito solicitando el citado consentimiento

[88] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Página 338.

en el que se ofrecía la posibilidad de oponerse y el plazo de un mes para comunicar dicha oposición[89].

Varios ejemplos españoles ilustran este punto[90]:

a. La AEPD no considera válida la información que se facilita empleando fórmulas tan amplias como las que se indican que los datos serán empleados para remitir "publicidad u ofertas" o "información sobre productos de su interés", pues en estos casos la información que se ofrece no permite que el afectado conozca el tipo de productos o servicios sobre los que se recibirá publicidad.

b. Procedimiento N° PS/00077/2004 tramitado ante la AEPD. Un menor, socio de un club infantil, suscribió, junto con su padre, un cupón inserto en la revista del club, en el que figuraba la siguiente leyenda "la finalidad de este fichero es mantener la relación con los socios del club infantil para comunicarles actividades culturales, formativas, deportiva y de ocio, y para el envío de promociones comerciales de productos o servicios que puedan resultar de interés". Con posterioridad a la entrega del citado cupón, el menor recibió una comunicación comercial en la que se publicitaba una ADSL y videojuegos.

   La AEPD sancionó los citados hechos, por vulneración del principio de calidad de los datos, al considerar que la leyenda no contenía la suficiente información acerca de las finalidades determinadas y que la cláusula empleada no permitía remitir cualquier tipo de información publicitaria. La resolución de la Agencia, fue posteriormente confirmada por la Audiencia Nacional, en su Sentencia de 27 de abril de 2006. Argumenta la referida sentencia que la expresión "promociones comerciales" no permite entender incluida cualquier clase de promoción comercial, sino que es necesario vincular el término "comercial" con el resto de finalidades del club y con las actividades generales de aquél y del público destinatario. No es posible considerar legítimo que dicha cláusula incluya y autorice cualquier clase de promoción comercial en relación a productos que pueden ser, incluso, contrarios a los intereses del público infantil y juvenil".

La Directiva 95/46/CE prevé como excepción al consentimiento cuando el tratamiento es necesario para la satisfacción del interés legítimo del responsable del tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado.

[89] RUBI NAVARRETE Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Ob. Cit. Página 10.
[90] RUBI NAVARRETE Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Ob. Cit. Página 10.

En España se considera como excepción al consentimiento, de acuerdo al artículo 6 n° 2 cuando "*los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado*".

Existe la posibilidad de que los titulares de los datos indiquen en la fuente pública que no desean que sus datos sean tratados con fines comerciales.

La Directiva exige que se informe sobre la identidad del responsable y la finalidad del tratamiento, por tanto, cuando se obtienen los datos de fuentes accesibles al público en las campañas publicitarias, deberá informarse de donde se obtuvo el dato.

En relación con lo previsto en la Directiva 2002/58/CE puede citarse el informe N° 0300/2009 y la resolución de 6 de noviembre de 2008, recaída en el expediente E/01544/2007 de la AEPD en que se analiza el procedimiento utilizado por Google para obtener el consentimiento de los usuarios del correo electrónico gratuito Gmail, en el cual se acepta que Google pueda asociar publicidad personalizada al contenido de los correos electrónicos que recibe dicho usuario. A través de hiperenlaces se lleva al documento de privacidad de los servicios de Google y se informa al usuario de Gmail que sus datos se tratarán con fines de publicidad. Al hacer clic en el botón Acepto se aceptan los Términos del Servicio como la Política de privacidad, lo que supone una aceptación expresa[91].

La LOPD y su reglamento reconocen el derecho de acceso y el derecho de oposición cuando los datos personales son tratados con finalidad de publicidad o de prospección comercial.

El derecho de acceso se reconoce en el artículo 30.3 LOPD "*en el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de la información a que se refiere el artículo 15*".

[91] RUBI NAVARRETE Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Ob. Cit. Página 9.

Se establece un reconocimiento expreso de este derecho en nuestro ámbito de estudio, no constituyendo una especialidad respecto de sus caracteres en la regulación que establece la LOPD; este derecho es confirmado en el ya citado artículo 50.1 del Reglamento de Protección de Datos (RPD) al disponer que "*el ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del Título III del Reglamento*".

El último de los derechos del interesado a que se refiere expresamente el artículo 30 LOPD (tratamiento con fines de publicidad y de prospección comercial) es el de oposición. Este derecho representa una novedad en el sistema jurídico de la protección de datos en España y deriva del artículo 14 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Posteriormente, el RPD ha desarrollado este derecho específicamente en el capítulo dedicado a los tratamientos para actividades de publicidad y prospección comercial (artículo 51 RPD)[92].

Una de las cuestiones más interesantes relacionadas con el derecho de oposición es el de las listas de exclusión, normalmente conocidas como "listas Robinson" [93], a las que ya nos referimos anteriormente.

Si bien el artículo 4.5 de la LOPD consagra que "*los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados*", el RPD en el artículo 49 dispone que "*los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad*".

Junto a la admisión de estas listas de exclusión el RPD prevé la puesta en funcionamiento de los denominados "ficheros comunes de exclusión del envío de comunicaciones comerciales". Se trata de la creación de listas de exclusión comunes a varios empresarios y que podrán presentar un ámbito general o sectorial, según afecten a la actividad publicitaria de todos o de un grupo de empresarios respectivamente. Su contenido, al igual que las listas individuales de exclusión, se ceñirá a "los *mínimos imprescindibles para identificar al afectado*" (artículo 49.1 RPD). Estas listas comunes deberán estar gestionadas

[92] DE LA VEGA GARCIA, Fernando L. "Datos personales y deberes del empresario en la publicidad". Ob. Cit. Página 32.
[93] DE LA VEGA GARCIA, Fernando L. "Datos personales y deberes del empresario en la publicidad". Ob. Cit. Página 34.

por un responsable, "*que podrá tratar los datos de los interesados que hubieren manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o de prospección comercial, cumpliendo las restantes obligaciones establecidas en la LOPD y el RPD*" (artículo 49.3 RPD)[94].

El empresario que desee utilizar los datos deberá:

1. Informar al interesado de la existencia de los ficheros comunes de exclusión, ya sean generales o sectoriales, la identidad del responsable, su domicilio y la finalidad del tratamiento de sus datos.

2. deberá consultar los ficheros comunes que pudieran afectar a su actuación, para evitar que sean objeto de tratamiento datos de los afectados que hubieran ejercido el derecho de oposición o negativa al tratamiento.

El 30 de marzo de 2012 se aprobó el Real Decreto-Ley 13/2012 por el que se transponen determinadas directivas comunicarías. Entre ellas, la Directiva 2009/136/CE que interpone modificaciones a la Ley 34/2002, que analizaremos en el capítulo actualidad[95].

## 3. ARGENTINA

Vamos a referirnos a Argentina porque es un país declarado adecuado a la Directiva de la Unión Europea y por ser su ley, al igual que la española, una de las fuentes de la norma uruguaya.

El artículo 27 de la Ley Nº 25.326 regula los archivos, registros o bancos de datos con fines de publicidad y establece:

"*En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios, o permitan establecer hábitos de consumos, cuando estos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.*

*En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.*

[94] DE LA VEGA GARCIA, Fernando L. "Datos personales y deberes del empresario en la publicidad". Ob. Cit Página 35.

[95] http://brosaabogados.blogspot.com.es/2012/04/modificaciones-para-adaptar-la-lssi-la.html pagina visitada 29 de marzo de 2012.

*El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo".*

El Decreto Reglamentario Nº 1558 publicado el 3 de diciembre del 2001 establece:

"*Artículo 27 – Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente para formular la oferta a los destinatarios.*

*Las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la Dirección Nacional de Protección de Datos Personales, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de Aplicación, implementarán, dentro de los noventa (90) días siguientes a la publicación de esta reglamentación un sistema de retiro o bloqueo a favor del titular del datos que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros.*

*En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información.*

*A fines de garantizar el derecho a la información del artículo 13 de la ley 25.326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la Dirección Nacional de Protección de Datos Personales, al que por estatuto adhieran obligatoriamente todos sus miembros. Al inscribirse, las cámaras, asociaciones y colegios profesionales deberán acompañar una nómina de sus asociados indicando nombre, apellido y domicilio.*

*Los responsables o usuarios de archivos, registros, bancos o bases de datos con fines de publicidad que no se encuentren adheridos a ningún Código de Conducta, cumplirán el deber de información inscribiéndose en el Registro a que se refiere el artículo 21 de la ley 25.326.*

*Los datos vinculados con la salud sólo podrán ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la*

*ley 25.326 y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no podrán transferirse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información de los artículos 6 y 11, inciso 1, de la ley 25.326 y la mención de su derecho a solicitar el retiro de la base de datos".*

Comenta el Dr. Pablo Palazzi a propósito de estos artículos que: "La ley argentina permite el marketing directo respetando la voluntad del destinatario de no recibir publicidad. No podrá ser de otra manera, ya que la prohibición directa de publicidad total, salvo algunas excepciones razonables, sería inconstitucional. (…) Como la norma está mal redactada han surgido dos teorías para interpretarla sobre la base de considerar que contempla dos supuestos distintos o uno solo. Una tesis sostiene que el punto y coma luego de la palabra "publicitarios" divide a los "datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios" de los datos que "permitan establecer hábitos de consumo". Estos últimos serían más personales y por ello requerirían el consentimiento del titular (si no se obtienen de fuentes públicas). (…) La reglamentación intentó aclarar esta confusión. A tales fines dispone que podrán recopilarse, tratarse y cederse datos con fines de publicidad *sin consentimiento* de su titular, cuando estén destinados a la formación de *perfiles determinados*, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios. Es decir, optó por considerar que los perfiles de consumo son distintos de los hábitos de consumo. Si se considera que esta distinción no está presente en la ley, el decreto reglamentario habrá excedido sus límites constitucionales alterando su sustancia"[96].

La reglamentación (artículo 27, Decreto 1558/2001) incluyó dos aspectos de las normas españolas (LORTAD, LOPD y real decreto 1332/1994). Primero, dispone que las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DINPDP, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de aplicación, implementarán, dentro de los noventa días siguientes a la publicación del decreto reglamentario, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de

[96] PALAZZI Pablo A. "La protección de los datos personales en la Argentina. Ley 25.326 de protección de datos personales y hábeas data comentada y anotada con jurisprudencia". Editorial Errepar. Argentina 2004. Páginas 191 y siguientes.

comunicación en particular, como el correo, el teléfono, el correo electrónico u otros[97].

La reglamentación también establece como debe informarse al titular de sus derechos y facultades.

La ley faculta a hacer marketing según lo dispuesto en el artículo 27.1 LPDP, pero en modo alguno ello implica que cualquier dato puede ser utilizado, ya que como bien señala la doctrina, en relación al artículo 27 de la LPDP: "Que los consumidores sean advertidos en oportunidad de proporcionar sus datos que estos van a ser ingresados en una base de datos de marketing constituye un requisito esencial para el respecto de sus derechos personalísimos. Que la ley autorice a las empresas a utilizar datos personales con fines lucrativos, es un aspecto de la libertad que merece ser respetado; si ello se realiza con deslealtad, y ocasiona molestias en la vida privada, esto es deshonesto, y a partir de la ley 25.326 es ilegal", (Gil Carbó, 2001)".

Esto implica que, quienes realizan marketing deben cumplir con el principio de finalidad y el principio de información y notificación de esa finalidad (artículos 4 y 6 de la LPDP)".

El Dr. Palazzi ilustra el tema objeto de estudio con una serie de casos que me ha parecido de interés citar[98]:

a. A comienzos de 1997, la empresa británica British Gas incluyó un folleto titulado "Sus derechos de protección de datos" con cada factura que envió a sus clientes. Este folleto establecía que British Gas comunicaría a sus clientes todos sus productos y servicios, y señalaba como intención hacerles saber asimismo de la existencia de productos de otras empresas y ceder información sobre sus clientes y otras empresas del grupo British Gas de modo que los clientes estuviesen informados. Si los clientes no querían recibir esa información podían excluirse devolviendo el formulario a British Gas. La autoridad de protección de datos entendió que el procedimiento no era legal, pues requería a los clientes recurrir a un procedimiento de "opt in" en vez de uno de "opt out", en especial pues estadísticamente era más probable que sólo unos pocos clientes estarían al tanto de haber recibido la noticia o conocer las consecuencias de no responder.

[97] PALAZZI Pablo A. "La protección de los datos personales en la Argentina. Ley 25.326 de protección de datos personales y hábeas data comentada y anotada con jurisprudencia". Ob. Cit. Página 193.
[98] PALAZZI Pablo A. "La protección de los datos personales en la Argentina. Ley 25.326 de protección de datos personales y hábeas data comentada y anotada con jurisprudencia". Ob. Cit. Página 194.

El tribunal de protección de datos, al analizar la licitud de este procedimiento tuvo en cuenta que la demandada era una empresa monopólica (en aquel entonces) y que el procedimiento de los datos para cederlo a terceros con fines de "marketing directo" era ilegítimo, a menos que se realizara con el consentimiento expreso del titular de los datos".

b. En un caso muy similar –*Midlands Electricity Plc c/ Data Protection Registrar* (1999)-, la autoridad inglesa había emitido una orden ante una queja de una persona que había recibido material de publicidad de la demandada cuyo envío no había consentido.

   La empresa había comenzado una campaña de marketing directo donde se incluía un folleto y una revista (*Homebright Magazine*), al remitir la factura a sus clientes. El folleto no sólo presentaba ofertas de *Midlands Electricity* sino también de terceras empresas como Boots y Midland Gas. El tribunal entendió que este tipo de procesamiento de datos personales era ilegal y que violaba el primer principio de protección de datos de la ley. Agregó que los clientes recibían la revista en forma general, sin haber tenido la oportunidad de consentir el uso de sus datos personales para esta finalidad.

   Respecto del tema del consentimiento en el área de marketing directo, el tribunal sostuvo en este caso que "…tanto con clientes existentes como con nuevos clientes, …consideramos que sea suficiente el envío al cliente de un folleto dándole una oportunidad de objetar el procesamiento de sus datos personales para finalidades distintas a aquellas relacionadas con la electricidad, tales como la preservación de energía …que hemos identificado como disponible para procesar datos sin consentimiento y sin ser ilegítimo… Sería suficiente para prevenir un procesamiento ilegal que los clientes sean informados que la demandada desee continuar enviándoles la revista conteniendo avisos de terceras partes que *Midlands* seleccionará o cualquier otra promoción que *Midlands* desee realizar, siempre que se les dé la elección de consentir o no o que no objeten que sus datos personales sea utilizados para dichos fines … Alternativamente, antes de que ese procesamiento tenga lugar, el cliente puede devolver a *Midlands* un documento u otro medio de comunicación donde indica su consentimiento, o por ejemplo, por no tildar un casillero de opt-out, u otro medio indicando que no objeta el procesamiento de sus datos personales para esos fines de marketing directo o promocionales" (Carey).

c. En igual sentido se litigó en la Argentina, un caso donde una entidad financiera invirtió el consentimiento y otorgó a sus clientes un plazo para solicitar que sus datos no fueran compartidos con empresas del grupo o terceros. En el caso, el juez denegó inicialmente la medida autosatisfactiva solicitada, pues consideró que coincidía con el objeto del

litigio (“Unión de Usuarios y Consumidores c/ Citibank”, Juzg. Com. N° 18, 29/9/03).

d. El derecho a no recibir comunicaciones de marketing por parte del titular no tiene relación con que los datos sean o no públicos. En realidad, pasa por otro aspecto del derecho a la autodeterminación informativa que incluye el derecho a no ser molestado con ofertas indeseadas, una vez que el titular hizo saber que no quería recibir más publicidad. Además, en otros ambientes como el digital, esta clase de marketing tiene molestias adicionales que superan la privacidad e incluyen costos económicos de pagar por recibir el mensaje, como sucede en el caso del spam (Palazzi, 2004ª).

e. Recordemos que no solo se viola la intimidad mediante la colocación de escuchas telefónicas, sino también a través de llamados telefónicos molestos o recurrentes, ya que no sólo se perturba la intimidad del hogar cuando se espía, sino también cuando se molesta el desenvolvimiento de las normales actividades de sus moradores sin justificación alguna (voto Dra. Medina, Capel. Civ. y Com. San Isidro, Sala I, 15/6/1999, “Wildemberg”, LLBA, 1999-1225).

La base de datos de marketing puede formarse también por datos “inferidos” de la información recogida legalmente. Puede suceder que mediante determinados programas de computación es posible crear categorías de personas en función del domicilio y otros datos que son públicos.

Así, sobre la base de datos que son de dominio público, como por ejemplo el domicilio, el ingreso promedio calculado de un determinado barrio o lugar de veraneo, es posible categorizar a la gente y elaborar este dato, sin acceder a datos individuales y personales de los registrados. Un programa puede entonces “presumir” determinados ingresos de estas personas y por ello no viola la LPDP[99].

También es posible realizar *cobranding* de ofertas de bienes conjuntos, siempre que la cesión no viole el artículo 11. Como estos datos son usados para realizar marketing y no para tomar decisiones que puedan afectar al registrado, no existe perjuicio alguno para el mismo y el tratamiento de esta clase de información es perfectamente legal, siempre que se realice con su consentimiento y en especial notificándole previamente, al recoger los datos, el uso que se hará de los mismos.

[99] PALAZZI, Pablo A. “La protección de los datos personales en la Argentina. Ley 25.326 de protección de datos personales y hábeas data comentada y anotada con jurisprudencia”. Ob. Cit. Página 197.

El concepto más convencional de co-branding es el de asociación de dos marcas con el fin de potenciar el valor y la rentabilidad de las mismas. Para que esta asociación resulte exitosa es de vital importancia la adecuación y complementación que se debe dar entre las mismas[100].

Mary Teahan comienza su presentación en el VII Seminario Nacional e Internacional "La protección de datos personales: una herramienta para el desarrollo económico" con una cita de la FCC de EEUU, 2010: "Históricamente, muchas empresas han utilizado datos personales 'offline' para formar perfiles de consumidores, lo que ha creado industrias billonarias". Partiendo de esta afirmación realiza una defensa del Marketing Directo, destacando los siguientes aspectos económicos, para la población: una opción de comprar a distancia a un precio menor y con un surtido mayor, crea empleos en el nuevo medio de ventas, mucho más efectivo en términos de costos que los medios masivos tradicionales de publicidad, especialmente para las PyMEs, por las mismas razones, los gobiernos y las empresas de servicios públicos a menudo lo usan. Destaca que la Ley de Protección de Datos Personales argentina es, básicamente, de "opt in" (optar por estar en la base de datos) y que la única excepción a esta regla se otorga al Marketing y que los datos necesarios para realizar la gran mayoría de las campañas de marketing se pueden tratar sin consentimiento previo del titular. Hace hincapié en que hay razones económicas para optar por el opt out y que el "no se puede nada" atenta contra el crecimiento del negocio propio, el desarrollo de la economía del país y la satisfacción de aquellos consumidores que quisiesen recibir ofertas[101].

Mary Teahan concluye su exposición afirmando que:

- El uso de datos personales para el marketing se convirtió desde hace mucho en una actividad económica importante.

- El advenimiento de Internet aumenta las posibilidades de este negocio y medio de comunicación.

- Este negocio genera beneficios al país, a la comunidad, además de los que produce para el comprador y vendedor.

- Hay un gran segmento de los consumidores que desea informarse y comprar vía esta modalidad.

[100] http://ricoveri.ve.tripod.com/ricoverimarketing2/id47.html Página visitada el 4 de agosto de 2011.
[101] TEAHAN, Mary. Presentación en el VII Seminario Nacional e Internacional "La protección de datos personales: una herramienta para el desarrollo económico". Buenos Aires, 22 de abril de 2010.

- En vez de obstaculizar el desarrollo de este mercado, los profesionales argentinos deberían buscar cómo alentarlo.

Por otra parte, hay que destacar que el Código de Ética de la Asociación de Marketing Directo e Interactivo de Argentina (AMDIA) nuclea a empresas, entidades de bien público y profesionales que promueven una práctica competente y ética del marketing directo e interactivo y de los tele servicios. Asume la responsabilidad de procurar que dichas actividades sean útiles y constructivas para el sector en particular y la comunidad en general.

## 4. URUGUAY

Respecto a nuestro país nos centraremos en dos aspectos: los derechos del consumidor y la protección de datos. No analizaremos aspectos referentes a la publicidad ilícita o engañosa, aunque esté específicamente regulada, porque entendemos que exceden el presente trabajo.

### 4.1 Derecho del consumidor

En Uruguay la Ley N° 17.250 del 11 de agosto de 2000 es la norma que regula las Relaciones de Consumo, la cual en el artículo 6 literal C bajo el acápite de derechos básicos del consumidor, establece que: "*La información suficiente, clara, veraz, en idioma español sin perjuicio que puedan emplearse además otros idiomas*".

Al respecto dice la Dra. Dora Szafir: "La situación actual del mercado, donde abundan los productos y servicios de alta tecnología, cuyo manejo es imposible por los usuarios sin la debida instrucción e información, hace necesaria la obligatoriedad de brindarla en forma clara, veraz y suficiente. De esa forma, se lograrán hombres bien informados, ciudadanos conocedores de sus derechos, en lugar de personas mal informadas que resultan ser súbditos de un mercado masivo"[102].

Dice el artículo 14: "*Toda información, aun la proporcionada en avisos publicitarios, difundida por cualquier forma o medio de comunicación, obliga al oferente que ordenó su difusión y a todo aquel que la utilice, e integra el contrato que se celebre con el consumidor*".

[102] SZAFIR, Dora. "Consumidores. Análisis exegético de la ley 17.189". Fundación de Cultura Universitaria. Montevideo, julio 2000.

Por su parte, el artículo 16 inciso 1° regula "*la oferta de productos o servicios que se realice fuera del local empresarial, por medio postal, telefónico, televisivo, informático o similar da derecho al consumidor que la aceptó a rescindir o resolver, "ipso-jure" el contrato. El consumidor podrá ejercer tal derecho dentro de los cinco días hábiles contados desde la formalización del contrato o de la entrega del producto, a su sola opción, sin responsabilidad alguna de su parte. La opción por la rescisión o resolución deberá ser comunicada al proveedor por cualquier medio fehaciente*".

## 4.2 Ley de Protección de Datos Personales

En nuestro país esta temática está regulada en la Ley Nº 18.331 de 11 de agosto de 2008, en el artículo 21, que originalmente establecía:

"*Artículo 21. Datos relativos a bases de datos con fines de publicidad. En la recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento*.

*En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.*

*El titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo*".

Así lo entiende el Grupo de Trabajo del Artículo 29 en el Dictamen 6/2010 de 12 de octubre de 2010, sobre el nivel de protección de datos personales en la República Oriental del Uruguay, cuando refiriendo a los principios adicionales considera en segundo lugar la Mercadotecnia directa y se establece que: "en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito".

"El Grupo de Trabajo considera que este principio está recogido en el artículo 21 de la LPDP, relativo a los casos de "recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas". "Así, tras señalar que "se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento" y reconocer el libre ejercicio, en todos los casos, del derecho de acceso, el último párrafo del artículo establece

claramente que “el titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo”.

Un aspecto interesante a destacar es el relativo al consentimiento y a las excepciones previstas en el artículo 9 literal c) de la ley N° 18.331.

Este aspecto ha sido analizado por el Grupo de Trabajo del Artículo 29 y en el informe ya referenciado se establece que: “El Grupo de Trabajo tienen también en cuenta las explicaciones de las autoridades uruguayas sobre la presunción de licitud del tratamiento del artículo 9, letra c), de la LPDP, en el que se establece que “*no será necesario el previo consentimiento cuando (…) se trate de listados cuyos datos se limiten en el caso de personas físicas, a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma*”.

Menciona el informe la aclaración realizada por las autoridades uruguayas, quienes entienden que: “la legitimidad derivada de este precepto no puede entenderse en ningún caso como algo diferente de los principios de legitimación, proporcionalidad y limitación del objetivo. Por tanto, aunque no sea necesario obtener el permiso de la persona afectada, el responsable sólo puede tratar los datos a que se hace referencia en este artículo cuando el tratamiento esté incluido en el ámbito de los objetivos explícitos y legítimos identificados y siempre que los datos sean adecuados, pertinentes y no excesivos con relación al objetivo señalado, sin que exista ninguna otra legitimación distinta al necesario cumplimiento de ambos principios”.

Otro aspecto relevante del Dictamen refiere a la interpretación del artículo 13 referente al deber de informar. Este punto fue objeto de aclaraciones porque se entendía que daba la impresión de que esa obligación sólo se refería a los supuestos en que el interesado facilite los datos voluntariamente y con su consentimiento. “(…) las autoridades afirman que tal obligación es absoluta, incondicional e independiente del motivo que legitime el tratamiento. La obligación de informar al interesado se aplica en todos los casos, independientemente de que los datos personales se soliciten a este mismo o a un tercero y de que el tratamiento se realice en virtud de la autorización del titular o de otra persona”.

“Las autoridades uruguayas aclaran igualmente que, si los datos se obtienen a través de un tercero mediante una comunicación de datos, el interesado deberá ser previamente informado asimismo de esta transferencia por la persona o la entidad que los comunique, con indicación de los destinatarios de los datos transferidos, con arreglo al artículo 13 de la LPDP”.

El inciso primero del artículo 21 fue modificado por la Ley Nº 18.719 de 20 de diciembre de 2011, agregándose únicamente la posibilidad de prospección comercial a texto expreso, quedando redactado de la siguiente forma:

*"En la recopilación de domicilios, reparto de documentos, publicidad, prospección comercial, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento"*.

Por tanto los datos pueden ser tratados cuando:

a) figuren en documentos accesibles al público,

b) sean facilitados por el titular o

c) sean obtenidos con su consentimiento.

Por otra parte el titular podrá ejercer los derechos de acceso, de retiro o bloqueo.

# CAPITULO IV

# MARKETING COMPORTAMENTAL EN LINEA

## 1. INTRODUCCION

Hemos analizado los conceptos generales en materia de marketing electrónico, las vulnerabilidades que pueden sufrir lo datos y finalmente, las regulaciones existentes en la Unión Europea, España, Argentina y nuestro país. Estamos en condiciones, de abordar, un tema sumamente específico, que convoca aspectos relativos a la publicidad y al marketing, pero que también puede resultar violatorio no solo de formas comerciales, sino de un derecho fundamental como es nuestra privacidad.

La libertad informática, como bien jurídico objeto de consumo en las sociedades avanzadas, no puede concebirse sin el contrapunto de la salvaguarda o defensa de los datos personales que afecten a la intimidad personal y familiar[103].

Paloma Llanesa comenta la Recomendación del Consejo Europeo de la Unión Europea de 19 de febrero de 1999 en lo que refiere al comportamiento de los proveedores de acceso en cuanto a la intimidad y privacidad de los usuarios en los siguientes términos:

"Así se les exhorta el uso de procedimientos adecuados y tecnologías disponibles, (especialmente aquéllas que se haya certificado que protegen la intimidad) para asegurar la integridad y la confidencialidad de los datos de sus usuarios así como la seguridad física y lógica de la red y de los servidores suministrados por la misma. El proveedor ha de informar a sus clientes de los riesgos que para la vida privada supone el uso de Internet, con carácter previo a que suscriban o comiencen a usar los servicios de acceso. La advertencia puede referirse a la integridad de los datos, a su confidencialidad, a los problemas de seguridad de la Red y a otros riesgos a su intimidad, como la acumulación o el registro de datos ilegales. También ha de informales sobre los medios técnicos que pueden usar legalmente para reducir los riesgos de seguridad en los datos y comunicaciones, así como la codificación legalmente disponible y las firmas digitales. En ese sentido, el Consejo recomienda que se ofrezcan dichos medios técnicos por el servidor a un precio orientado al coste y no disuasorio. Los ISP, antes de aceptar suscripciones y conectar a los usuarios a Internet, han de informarles sobre las posibilidades de acceder a Internet anónimamente y a usar sus servicios y pagar por ellos de forma

[103] ALVAREZ-CIENFUEGOS SUAREZ José María. "La defensa de la intimidad de los ciudadanos y la tecnología informática". Ob. Cit. Página 15.

anónima (por ejemplo, con tarjetas de acceso de prepago). En los casos en que el anonimato total no sea adecuado a causa de las restricciones legales, el ISP ha de facilitar la posibilidad de usar seudónimos, informándoles de los programas que permitan navegar de manera anónima, diseñando incluso su sistema de modo que evite o minimice el uso de datos personales"[104].

La recogida, procesado y almacenamiento de los datos de los usuarios ha de limitarse a los supuestos en que sea necesario para objetivos explícitos, especificados y legítimos. Los ISP han de velar porque no se produzca interferencia alguna de las comunicaciones, a menos que la interferencia esté prevista por ley y sea llevada a cabo por la autoridad pública, suministrando ésta las salvaguardas necesarias para asegurar la protección de los datos. En igual sentido, los ISP no han de transferir los datos de sus usuarios a no ser que la transferencia esté prevista por ley, ni almacenados por más tiempo que el necesario para conseguir el objetivo de procesamiento, ni usarlos para autopromoción o publicidad, a menos que el usuario, tras ser informado, no se haya opuesto. En caso de procesamiento de datos de tráfico o datos confidenciales, habrá el ISP de solicitar el consentimiento explícito del usuario[105].

El Consejo hace responsable a los ISP del correcto uso de los datos. Con este presupuesto, en la página de introducción realiza una declaración clara sobre el sistema de respeto a la intimidad y a la vida privada, hipervinculada a una explicación detallada de la política de uso de los datos de carácter personal.

El editor de una página debe informar a los usuarios, con carácter previo al uso del servicio o al acceso a la información, qué datos recoge, procesa y almacena, de qué modo, con qué propósito y por cuánto tiempo los conserva.

A petición de los usuarios, los ISP han de corregir los datos erróneos de manera inmediata, procediendo directamente a su borrado si son excesivos, fuera de fecha o si no se necesitan por más tiempo. Esto incluye la paralización del procesado de los mismos si el usuario se opone.

Los ISP habrán de notificar la voluntad así manifestada de los usuarios a las terceras personas a las que haya comunicados dichos datos y evitar la acumulación secreta de datos. Por último, el Consejo recuerda a los ISP que han de notificar a los usuarios la información que de ellos tienen, y que la misma debe ser exacta y reflejar la conservada hasta la fecha[106].

[104] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Bosch. Barcelona, abril 2000. Página 261.
[105] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación. Ob. Cit. Páginas 261 y 262.
[106] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Ob. Cit. Página 262.

La gratuidad de los diferentes servicios en Internet, que funciona de manera generalizada, a excepción del software y la pornografía, obliga a buscar otros medios para que el negocio sea viable, y la respuesta se encontró en la publicidad como fuente de ingresos necesaria para el mantenimiento y administración de los sitios web.

Nadie se cuestiona pagar por leer un periódico en papel, pero pocos pagarían por leerlo en su edición digital. Es evidente, pues, que ofrecer gratis en Internet lo que se cobra en el mundo analógico viene produciendo una migración a la Red que ha de compensarse económicamente. Internet, técnicamente, proporciona, junto con el acceso gratuito a los contenidos, los elementos técnicos que hacen posible los anuncios personalizados o a la carta, gracias a la monitorización de la navegación que permite crear perfiles virtuales del consumidor muy cercanos a su naturaleza más profunda"[107].

El Convenio 108 del Consejo de Europa de 28 de enero de 1981, referenciado en el capítulo anterior, intenta mantener un difícil equilibrio entre los intereses comerciales que subyacen en la transmisión de las bases de datos y la efectiva protección éstas.

El propio Preámbulo del Convenio trasluce esta dicotomía, pues tras recordar la importancia que tiene la protección de los derechos y libertades fundamentales de cada ciudadano –especialmente el respeto a su vida privada-, reconoce la necesidad de conciliar los valores fundamentales de respeto a la vida privada con el de la libre circulación de la información entre los países. El artículo 11 del convenio permite a los Estados parte que cada uno de ellos pueda conceder a sus ciudadanos una protección mayor que la prevista en el convenio[108].

El marketing directo, la publicidad en Internet, la captura de datos con fines de publicidad han sido temas que he abordado con anterioridad, en diversas oportunidades.

Pero, tratándose de un aspecto tan crítico de la vida comercial, del contacto comercial inicial, de la forma en que podemos llegar a los consumidores, como obtener nuevos clientes y acceder a un nuevo nicho de mercado, cuando toda la información se encuentra disponible en Internet y existe la tecnología para procesarla y utilizarla de la forma más provechosa, sigue planteando permanentes desafíos[109].

---

[107] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Ob. Cit. Página 263.

[108] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Ob. Cit. Página 275.

[109] VIEGA María José. "El marketing comportamental en línea desde la óptica de la protección de datos". Ponencia presentada al Primer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática. CIIDDI 2011. Mar del Plata, Argentina. 1, 2 y 3 de diciembre de 2011.

El nombre marketing comportamental en línea es sin duda peculiar, al punto que si buscamos en el diccionario de la Real Academia Española la palabra "comportamental", nos dice que no se encuentra en éste. Marketing comportamental es la traducción que se ha hecho a la expresión "*on line behavioral advertising*".

Ingresando en el corazón del presente trabajo, previo análisis de los presupuestos que entendimos necesarios a los efectos de arribar a esta problemática, debemos tener presente que este es un tema con poco desarrollo doctrinario, que plantea más preguntas que respuestas. Desde el punto de vista de los proveedores está clara la gran utilidad que presenta, las dudas surgen frente a los derechos de los consumidores, concretamente relacionados con la violación de su privacidad.

En una ponencia realizada en el año 2002 sobre "Privacidad en Internet" decía: "Hoy por hoy se entiende que la vida privada no se limita a la intimidad, sino que este concepto ha sido sustituido por uno más general como es el de privacidad. Internet es una amenaza en la difusión de elementos relativos al individuo y un desafío para el derecho no solo en este tema puntual sino a las repercusiones que tiene en general la globalidad"[110].

Y agregaba que "La Red es un medio de comunicación polifacético, debido a la existencia de múltiples medios para distribuir información. Ellos son: el correo electrónico, los boletines, los foros de discusión y también la información presente en la www. Para enfrentar este desafío se deben tener en cuenta los siguientes elementos:

a) En primer lugar que la infraestructura de Internet está basada en datos personales (IP).

Una discusión muy interesante que se ha planteado es si un numero IP es un dato personal (o dicho número en un instante, porque hay IP variables y rotativas), y si se puede acceder a dicha información sin el consentimiento del usuario.

La Agencia de Protección de Datos Española[111] ha interpretado de esta manera y ha declarado a la dirección IP como dato personal.

¿Es un dato personal o es como dicen los técnicos simplemente un número referenciador?, ¿este número IP puede llegar a considerarse un bien?

[110] VIEGA María José. "Privacidad en Internet". Derecho Informático. Tomo II. Fundación de Cultura Universitaria. Páginas 235 y siguientes.
[111] https://www.agpd.es/index.php?idSeccion=390

El Dr. José Luis Barzallo entiende[112] que la dirección IP es un identificador y una dirección de correo electrónico y que no cumple con los elementos necesarios para considerase como un dato personal. Sin embargo algunas legislaciones, que han avanzado con el tratamiento del tema, ya lo han considerado como tal y lo protegen. Podría considerarse como un dato personal, pero no de aquellos sometidos a protección por ser privados, confidenciales o sensibles. Tampoco debemos dejar de lado que el dato personal fue desarrollado por la doctrina de defensa de los derechos humanos para el individuo, entonces las personas jurídicas tienen otras figuras protegidas por otras ramas del derecho como la propiedad intelectual. Podría ser considerado como un bien cuando es fijo y cumpliendo requisitos como una titularidad que alguien tenga sobre ese bien.

Sobre las opiniones del Dr. Barzallo respecto a las personas jurídicas es interesante destacar que, la Ley N° 18.331 consagra a la protección de datos como un derecho humano reconocido en la Constitución, pero sin embargo, lo hace extensible a las personas jurídicas en cuanto le es aplicable.

Con relación a la dirección IP debemos ser más precisos y preguntarnos ¿qué sucede si es un numero IP fijo?, porque en este caso identifica a un usuario en el sistema. Tengamos presente que en realidad lo que identificamos es una máquina, ahora bien, si la misma es usada por un único individuo, ¿no estaríamos ante un dato de ese "individuo" y por tanto un dato personal?

El Dr. Felipe Fontes[113] entiende que el número IP, es equiparado a la dirección de una persona, por tanto no deja de ser un dato personal, pues la dirección, en su opinión lo es y sólo puede ser divulgado con la autorización del propietario o, por supuesto, por decisión judicial y a veces por cuestión de interés público.

Andrés Guadamuz González[114] explica que en el Reino Unido, las direcciones IP son ahora consideradas datos personales de acuerdo con la legislación de datos personales y la legislación de datos electrónicos. Esto es con respecto a la interpretación que se le esta dando a la sección 14 con respecto a "location data". Se interpreta ahora que las direcciones IP pueden cumplir este requisito. Con respecto a las direcciones IP en general, el Comisionado de Información (el ente regulador en Reino Unido), ahora interpreta que como la dirección IP puede usarse para identificar usuarios y es lo que hacen en Internet, se debe considerar como dato personal. De hecho, en Europa en general se piensa que las direcciones IP deben ser considerados datos personales[115].

---

[112] BARZALLO José Luis. Comunidad alfa-redi www.alfa-redi.org
[113] FONTES Felipe. Comunidad alfa-redi www.alfa-redi.org
[114] GUADAMUZ GONZALEZ, Andrés. Comunidad alfa-redi www.alfa-redi.org
[115] http://www.informationcommissioner.gov.uk/cms/DocumentUploads/what%20are%20personal%20data%20research.pdf

Según Roberto L. Ferrer Serrano[116]: "al menos desde el punto de vista de la normativa española, es evidente que puede ser considerado un dato personal, igual da que sea IP fija o no, porque en este último caso, siempre hay medios para asociarla a un usuario concreto. En su opinión, no significa que siempre vaya a ser un dato personal porque su naturaleza de dato personal deriva de su posibilidad de asociarlo a una persona identificada o identificable ex artículo 3 LOPD. *Artículo 3. Definiciones. A los efectos de la presente Ley orgánica se entenderá por a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables".* Por eso entiende que solamente dejará de ser un dato de carácter personal cuando por cualquier circunstancia no sea posible vincularlo a una persona.

b) Un segundo elemento se refiere a los instrumentos técnicos utilizados, software de navegación, por ejemplo, que envían más información de la requerida para realizar una conexión.

c) Y en tercer lugar la cantidad de datos que nos solicitan para realizar actividades comerciales en línea".

En la misma línea que éste último punto, Paloma LLanesa menciona lo siguiente: "En las visitas a las páginas web para hacer uso de un servicio o adquirir algún producto se suelen solicitar ciertos datos personales innecesarios. En la mayor parte de los casos, facilitamos estos datos para usar gratuitamente algún servicio, como por ejemplo correo electrónico en web, acceso a determinada información o almacenamiento de webs. Por lo tanto, es evidente que "pagamos" inconcientemente la información o servicio con nuestros datos personales. En los casos en que los datos son necesarios para la venta del producto o para la prestación del servicio de pago, corremos el riesgo de que los mismos sean utilizados para fines diferentes de aquellos para los cuales fueron recabados: confección de publicidad personalizada, rastreo de intereses y aficiones, comercialización de los mismos a terceras personas, etc. Es evidente que hay una ausencia de consciencia del consumidor del acto de facilitar los datos en ambos supuestos, pues no hacemos un verdadero acto de voluntad de cesión de los mismos ni conocemos que tienen un valor económico en sí mismos. Son pocos los que son conscientes de este hecho económico y ya se han dado casos en la Red de contraprestaciones económicas para facilitar los datos personales"[117].

Hemos destacado en un trabajo anterior tres elementos de fundamental importancia en Internet para el manejo de datos, que recopilan y envían

[116] FERRER SERRANO, Roberto. Comunidad alfa-redi www.alfa-redi.org
[117] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Ob. Cit. Página 264.

información sin que los usuarios estemos informados. Mencionaba entonces a las cookies, los navegadores y los contenidos activos.[118]

1) Cookies: son fichas de información automatizada, las cuales se envían desde un servidor web al ordenador del usuario, con el objetivo de identificar en el futuro las visitas al mismo sitio.

La Agencia de Protección de Datos española, en sus "Recomendaciones a Usuarios de Internet" de julio de 1997, define las cookies como el "conjunto de datos que envía un servidor Web a cualquier navegador que le visita, con información sobre la utilización que se ha hecho, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. Esta información se almacena en un fichero en el directorio del navegador para ser utilizada en una próxima visita a dicho servidor".

"El uso de cookies es un instrumento de obtención de información para el administrador de un servidor con fines no estadísticos, sino más bien de índole comercial. Conforme la definición de la APD, el archivo cookie puede contener la dirección IP del usuario, lo que permitiría identificarlo inmediatamente, de hacer uso de una dirección IP fija cuando el usuario tenga asignada esa dirección IP. Las IP dinámicas no trazan una relación inmediata entre el usuario y la IP, si bien el ISP que le dio acceso a la red conoce la identidad del usuario al que facilitó la dirección IP en un determinado día y hora, gracias a que los datos de la sesión se graban en el *log* del sistema. Las IP dinámicas evitan, en principio, la identificación del usuario por los servidores de las páginas visitadas, no así por su propio proveedor de acceso"[119].

Respecto al término y su conceptualización Trinidad Vazquez Ruano dice que la Directiva 2002/58/CE en el Considerando 25 ha optado por denominarlos *chivatos*. Si bien, literalmente, el término inglés "cookie" significa galleta, nos referimos a ellos en género masculino porque de su definición se extrae que son: fragmentos o ficheros de texto (* .txt) que se envían a un navegador por medio de un servidor web para registrar las actividades de un usuario en el determinado web site. Este tipo de archivos fue inventado por Lou Montulli (antiguo empleado de Netscape Communications). Desde el punto de vista técnico son archivos con una capacidad de 4 kbytes que se almacenan en el disco duro del ordenador del usuario, lo que permite al servidor no sobrecargarse hasta que se cierra el navegador o en la memoria RAM. Para ver los archivos cookies se puede utilizar un editor de texto. En concreto, los usuarios de Netscape en Windows, el fichero se llama cookies.txt, y se encuentra en la misma carpeta que Netscape. Los usuarios de Macintosh

[118] VIEGA María José. "Privacidad en Internet". Derecho Informático. Tomo II. Fundación de Cultura Universitaria. Páginas 235 y siguientes.
[119] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Ob. Cit. Página 267.

pueden encontrarlo en la carpeta de Netscape, en Sistema/Preferencias. Por su parte, Internet Explorer crea ficheros separados por cada cookie y los almacena en carpetas llamadas Cookies o ficheros Temporary Internet[120].

2) Navegadores: envían más información que la necesaria para establecer una comunicación, como por ejemplo el tipo y lengua del navegador, qué otros programas se encuentran instalados, cuál es el sistema operativo del usuario, cookies, etc.

"Matizamos que se hace referencia a la información que el programa de navegación de un usuario facilita por la mera conexión a la Red y que es susceptible de calificarse como personal, en tanto que identifica al usuario en forma directa o indirectamente. Sin embargo, en este último supuesto, si los datos facilitados no se relacionan con los anteriores a efectos de conseguir el perfil de un determinado usuario on line y, por tanto son considerados de forma aislada, no cabría afirmar que se trata de información personal en los términos de la norma. Pues son datos que en ocasiones se utilizan a efectos estadísticos o de cómputo, sin interesar las características ni rasgos particulares del sujeto titular de los mismos que se ha conectado a Internet. Los datos que no pueden calificarse como datos de carácter personal y que sólo se utilizan a efectos estadísticos, tales como: las páginas web visitadas o el número de clics efectuados, son calificados en términos de marketing como "datos agregados"[121].

Como veremos más adelante, esta opinión no se comparte totalmente.

3) Contenidos Activos: ejecución de programas con este tipo de contenidos, como por ejemplo el Java y el ActiveX. Si bien los hemos considerados por separados, hay autores que los denominan "cookies activas" que pueden ser ejecutadas de forma no consentida, instalándose en el disco duro del ordenador para controlar los datos personales que existen en él y aprovechan otras cookies ya instaladas que revelen los gustos del usuario.

Estos temas son tan actuales como en el momento en que los exponíamos en las Jornadas del Instituto de Derecho Informático del año 2001, si bien, por ejemplo, el tema de las cookies se ha regulado en la Unión Europea recientemente, existiendo diferentes puntos de vista en los países europeos a la hora de su incorporación y diferentes consideraciones en cuanto a su implicancia a nivel internacional.

En el Considerando 25 de la Directiva 2002/58/CE se señala que las "*cookies pueden constituir un legítimo instrumento y de gran utilidad, como por ejemplo,*

[120] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Página 159.
[121] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit.. Página 160.

*para analizar la efectividad del diseño y de la publicidad de un sitio web y para verificar la identidad de los usuarios partícipes en una transacción en línea. Y añade que en aquellos casos en los que tengan un propósito legítimo, como el de facilitar los servicios de la sociedad de la información, debe facilitarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto para garantizar que los usuarios estén al corriente de la información que se introduce en el equipo terminal que están utilizando*…".

También es actual el tema de los navegadores y la información respecto al sistema operativo. Tal es así, que en el evento Segurinfo 2011 que se llevó a cabo el 2 de junio en Montevideo, Sebastián Bortnik expuso sobre "Malware y cibercrimen en Latinoamérica"[122] y comentaba que el China online game ataca a nivel mundial, todos los países están infectados, excepto en China. Esto se debe a que el código malicioso tiene una línea que establece que si el sistema operativo está en chino no lo infecta.

Esta información es transparente para nosotros, no tenemos conciencia de su manejo ni de los riesgos que ello implica. Pero se han agregado potenciales amenazas, desde los blog donde escribimos nuestras opiniones o contamos las más diversas experiencias, hasta las redes sociales, que es suficiente para dimensionar su potencialidad el hecho de que Facebook se lanzó en febrero de 2004 y llegó en mayo de 2011 a 600 millones de usuarios.

Pero, además de las herramientas lícitas que permiten la recolección de datos personales, encontramos la instalación de otros elementos, ilegítimos y dañinos en la mayoría de los casos, como por ejemplo los citados por Trinidad Vázquez, habiendo hecho referencia a algunos de ellos con anterioridad, al tratar el tema de las amenazas[123]:

a. Spyware: son aplicaciones que obtienen datos sobre una persona u organización sin su conocimiento y con posterioridad se facilitan a entidades empresariales para que sean utilizados con fines publicitarios o a las autoridades en una investigación criminal.

b. Web bug: suelen insertarse en una página web o en una cuenta de correo electrónico por terceras personas para obtener información sobre los usuarios de la página en cuestión o de los correos electrónicos que se intercambian.

c. Identificadores ocultos: consisten en unas indicaciones específicas de lenguaje de marcación de hipertexto (HTML) hechas al navegador, pero que cuando se visualiza una determinada página en Internet se hallan ocultos.

---

[122] VIEGA, María José. Comentario de la conferencia realizada en el blog. http://mjv.viegasociados.com

[123] VAZQUEZ RUANO, Trinidad. "La protección de los destinatarios de las comunicaciones comerciales electrónicas". Ob. Cit. Página 159.

d. Gusanos: son un código maligno que se propaga a través de correo electrónico y se multiplica en cada uno de los equipos informáticos infectados, no eliminando información, sino afectando un amplio elenco de recursos informáticos.

e. Sniffer: son programas que recaban numerosa información que circula en la Red de forma que ejecutados en una red local permiten obtener pares (usuario-contraseña) de modo fácil.

## 2. CONCEPTO DE MARKETING COMPORTAMENTAL

La Comisión Federal de Comercio en los EE.UU. define el Online Behavioral Advertising (en adelante OBA) como "el seguimiento de las actividades de los consumidores en línea a través del tiempo -incluyendo las búsquedas que ha llevado a cabo el consumidor, las páginas web visitadas y el contenido que ha visto- con el fin de ofrecer publicidad dirigida a los intereses de los consumidores individuales".

La definición de la Comisión Federal de Comercio no es idéntica a la definición dada por el Grupo de Trabajo del Artículo 29 que analizaremos seguidamente, pero son muy similares.

Según Phil Lee[124] el objetivo del OBA es servir a la publicidad que es más relevante para los intereses de los consumidores y, al hacerlo, aumenta el *click-through* en esos anuncios. Algunos estudios han sugerido que los anuncios dirigidos actualmente tienen un *click-through rate* de aproximadamente 6.700% más alto que el que ordinariamente tiene una red.

*Clic-through* es la unidad de medida bruta de la eficacia de un banner publicitario la cual es obtenida al calcular todas las entradas a un sitio web como resultado de hacer click en el citado banner. El *click-through ratio* (tasa de pulsación pasante) es la unidad de medida neta de la eficacia de un banner. La proporción de clics se obtiene dividiendo el número de usuarios que pulsaron una pieza publicitaria -banner- por el número de impresiones mostradas de la misma, expresado en tanto por ciento[125].

Dar la definición de la FTC es para destacar que esto no es un problema de la Unión Europea, sino que un problema internacional y está atrayendo tanta atención sobre los EE.UU. como en Europa. La industria quiere una solución

[124] LEE Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.
[125] http://www.serviciosadomicilio.cl/diccionario-internet/click-through.htm Página visitada 14 de julio de 2011.

armonizada y coordinada para hacer frente al tema de regular o auto-regular la OBA.

Phil Lee[126] entiende que el peligro es la falta de armonía entre Europa y los EE.UU. Europa por un lado está inclinada hacia el opt in y EEUU por el otro, inclinado hacia una especie de opt out. Pero también se está viendo la falta de armonía dentro de Europa en sí misma.

## 3. ASPECTOS CONCEPTUALES Y TECNICOS

El Dictamen 2/2010 sobre publicidad comportamental en línea del Grupo de Trabajo del Artículo 29 parte de la base que la publicidad en línea es una fuente esencial de ingresos para un amplio abanico de servicios en línea y es un factor importante en el crecimiento y la expansión de la economía de Internet. Pero, no obstante ello, la publicidad comportamental suscita graves inquietudes en materia de protección de datos y privacidad.

### 3.1 Clasificación del marketing en línea

Además de los conceptos sobre marketing electrónico expuestos en el capítulo primero, me interesa destacar en este punto concreto, que existen diferentes métodos para crear anuncios en línea, los cuales pueden clasificarse en:

a) Publicidad contextual: es la que se selecciona en base al contenido que está viendo el sujeto en un momento determinado. Puede realizarse a través de una búsqueda concreta o de la dirección IP si ésta indica la ubicación geográfica.

b) Publicidad segmentada: es la seleccionada en base a las características conocidas del sujeto, como por ejemplo la edad, el sexo, la ubicación, etc., las cuales son proporcionadas por el usuario al inscribirse o registrarse.

c) Publicidad comportamental: es la publicidad basada en la observancia continuada del comportamiento de los individuos, que busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento.

[126] LEE Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

Las dos primeras dan una idea momentánea de lo que hace una persona, mientras que la comportamental puede dar un informe detallado de la vida en línea de ésta.

### 3.2 Sujetos que participan en la publicidad comportamental

Tenemos diferentes sujetos involucrados en la publicidad comportamental, los cuales poseen diferentes intereses y juegan diferentes roles. Ellos son:

a) Proveedores de redes de publicidad: son quienes conectan a los editores con los anunciantes.

b) Anunciantes: quienes desean promocionar un producto o servicio ante un sector de mercado.

c) Editores: los propietarios de los sitios de internet que pretenden obtener ingresos vendiendo espacio para mostrar los anuncios.

### 3.3 Modalidades de la publicidad comportamental

Para realizar publicidad comportamental se utiliza tecnología de rastreo, como es el caso de las cookies, el control de contenidos de los usuarios y las tecnologías que utilizan las direcciones IP. Como vimos, éste es un tema que lleva años sobre el tapete y que hoy día a tomado especial vigencia y se están buscado soluciones que protejan a los usuarios.

#### 3.3.1 Las cookies

La tecnología más utilizada son las cookies de rastreo que se instalan en el terminal del usuario, consiste en un código alfanumérico que se almacena y recupera posteriormente y permite que el proveedor reconozca a un antiguo visitante que va construyendo un perfil. Normalmente las cookies las coloca el editor y no el propietario del sitio, por lo que se suelen llamar “cookies de terceros”.

Es posible caracterizar a las cookies de la siguiente forma[127]:

a) Están ligadas a un dominio: solo puede leerlo o modificarlo el sitio de internet procedente de un dominio similar.

[127] VIEGA María José. “Marketing comportamental en línea”. Conferencia dictada en las Jornadas Académicas del Instituto de Derecho informático. Montevideo, 15 y 16 de junio de 2011.

b) Tienen vidas útiles distintas. Encontramos las “Cookies persistentes” duran mucho tiempo o hasta que se las borre manualmente.

c) Si la persona utiliza diferentes buscadores, las cookies serán diferentes para cada buscador.

Las “Flash cookies”, también denominadas por la prensa como “super cookies”, poseen técnicas reforzadas de rastreo y no pueden borrarse con la configuración tradicional de privacidad de un buscador. Se utilizan para restaurar las cookies tradicionales. Esta práctica se conoce como *respawning* (reproducción).

“Algunos programas navegadores asignan de forma automática el nombre del usuario al fichero que se genera como *cookie*. De esta manera, el nombre del fichero puede estar formado por el nombre del usuario, un símbolo de separación y el nombre del servidor que ha dado instrucciones para generar el archivo *cookie*. Para que esta asignación pueda producirse, el navegador debe haber sido previamente personalizado por el usuario, en el momento de la instalación o con posterioridad. Si ello no se produce, el contenido del *cookie* no podrá ser considerado como personal, ya que no podrán ser asociados a una persona identificada. No obstante, el archivo cookie puede contener la dirección IP del usuario. En este caso su identidad podría ser obtenida si utiliza una dirección IP fija, siempre que sea notorio el uso de dicha IP fija por un usuario determinado”[128].

Esta opinión no se comparte en la medida que está en contraposición con la definición dada de las cookies cuando mencionábamos que se trata de un código alfanumérico y no está asociado al nombre de la persona, pero sin embargo, este hecho no le quita su carácter de invasiva. Con relación a la IP ya comentamos las diferentes posiciones y nos adherimos a la concepción de que estamos ante un dato personal.

### 3.3.2 Control del contenido de los usuarios

No hay nada nuevo bajo el sol, más de 10 años atrás encontramos antecedentes de este tema, aunque cambien las tecnologías, la problemática es la misma, por lo que aportamos el siguiente ejemplo:

“Recientemente, uno de los mayores proveedores de albergue gratuito, Georcities, vio cómo la “Federal Trade Comisión” (FTC) estadounidense iniciaba un procedimiento por el uso indebido de los datos facilitados por sus usuarios. Georcities forma una comunidad virtual de más de dos millones de miembros que se divide temáticamente en diversos barrios en donde los

[128] RIVAS ALEJANDRO, Javier. “Aspectos jurídicos del Comercio Electrónico en Internet”. Editorial Aranzadi. Segunda reimpresión, octubre 2000. Página 51.

usuarios albergan sus páginas de forma gratuita. Para dar de alta una página, resulta preceptivo el rellenado de un formulario en el que se solicitan datos personales, unos de carácter obligatorio y otros de carácter opcional. Georcities introdujo la información obtenida en una base de datos que incluía las direcciones postales, direcciones de correo electrónico, áreas de interés del usuario, ingresos, formación, sexo, estado civil y ocupación. Este fichero informatizado permitía a Georcities, en opinión de la FTC, generar perfiles de usuarios y ceder sus ficheros de datos debidamente segmentados a terceros. Georcities, en definitiva, vendía la base de datos de sus usuarios de manera inconsentida a terceros con fines comerciales. La cuestión se solventó a mediados de 1998, llegando a un acuerdo por el que se ponía fin al procedimiento iniciado por la FTC a cambio de que Georcities publicase en su página web un aviso sobre intimidad, explicando a los usuarios qué información estaba siendo obtenida de los mismos y con qué propósito, a quien sería transmitida y cómo se podía acceder a dichos datos y exigir su cancelación. Demás, Georcities venía obligado a obtener consentimiento paterno antes de obtener información de usuarios menores de 13 años"[129].

En esta modalidad, la red de publicidad se asocia con un ISP para controlar el contenido de las búsquedas del usuario e insertar cookies de rastreo en todo el tráfico no encriptado de webs.

Un ejemplo de ello es la empresa Phorm, que utiliza tecnología Webwise y ofrece un servicio de publicidad comportamental que usa la inspección por paquetes en profundidad para examinar las páginas que visitan los usuarios. Phorm realizó acuerdos con los ISP para poder realizar el servicio. El Grupo de Trabajo del Artículo 29 aclara que no tiene conocimiento que esta tecnología se esté aplicando en la Unión Europea, pero que los problemas jurídicos van más allá de la protección de datos y exceden el ámbito del Dictamen 2/2010.

¿Cómo se crean los perfiles de usuario?

Existen dos modalidades, pero pueden combinarse:

a) Perfiles predictivos: se infieren determinadas características basadas en la observación del comportamiento del usuario.

b) Perfiles explícitos: son creados a partir de datos personales proporcionados por el usuario en Internet.

### 3.3.3 Localización física

[129] LLANEZA GONZALEZ Paloma. "Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación". Ob. Cit. Página 260.

Otra forma de determinar un perfil del usuario es a través de la localización física, que puede deducirse de la dirección IP y de los puntos de acceso wifi.

Phil Lee[130] manifiesta que vale la pena recordar que, aunque la opinión del Grupo de Trabajo se centra en redes de anuncios de terceras partes y cookies en realidad hay diferentes tipos de OBA. Y establece los tres tipos principales que se ven típicamente, cuyo análisis desarrollamos a continuación.

En primer lugar, es cuando un editor del sitio web, pone sus "cookies" en sus propios sitios web y recoge información sobre los visitantes y utiliza esa información para orientar los anuncios a los visitantes en su propio sitio. Eso es bastante común, se puede pensar en ello por ejemplo, cuando se visita Amazon y Amazon le da recomendaciones de libros basados en la navegación anterior y el historial de compras. Y curiosamente, en realidad, es algo que la gente probablemente ni siquiera pensaba en llamar OBA, hasta hace más o menos un año.

En el otro extremo del espectro, está la vigilancia del tráfico de los ISP o la inspección profunda de paquetes y esta es tecnología de punta desplegada por organizaciones como Phorm. Lo que ocurre allí es que el proveedor de tecnología OBA intercepta todo el tráfico que pasa a través de un proveedor de servicios de Internet y recoge los detalles sobre las páginas web que se utiliza y los hábitos de navegación de los clientes, y el ISP usa esa información para orientar los anuncios en sitios web de la asociación y es lo que está en el lado más intrusivo del espectro de la publicidad de comportamiento. Se puede pensar en esto como que tu cartero inspeccione tu correo en el mundo real (para diferenciarlo del ciberespacio).

Redes de anuncios de terceras partes: una especie de modelo de anuncio de Google se encuentra en algún lugar entre los dos extremos del espectro. Y lo que sucede es que un proveedor de la OBA coloca cookies en sitios web de un asociado para recopilar información sobre los visitantes de esos sitios con el objetivo de generar anuncios a los usuarios.

Ahora, históricamente, una gran parte del debate en torno a OBA inició el interés sobre formas de la tecnología en el Reino Unido en 2008. Lo que ocurrió allí fue que Phorm desarrolló un ensayo de su tecnología con un proveedor servicios de Internet -British Telecom- y lo hizo sin hacer ningún tipo de declaraciones a los usuarios. La prensa lo llamó un tipo de "ensayos secretos". Cuando salió a la luz, los usuarios estaban naturalmente disgustados de que su tráfico estuviese siendo monitoreado sin su conocimiento y sin su consentimiento. Y recibió mucha atención adversa de la prensa y todo lo que

[130] LEE Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

siguió después, todo el debate y la regulación europea posterior es la forma en que realmente comenzó esta historia.

Otro aspecto que me interesa destacar es el uso para publicidad de los datos existentes en las redes sociales.

El usuario de las redes sociales puede intentar controlar, con la configuración de su perfil, qué datos quiere que sean públicos y para quién, pero la cuestión se plantea con la información que tiene de él el prestador de servicios de redes sociales y los usos que de ella se hagan así como la información publicada por terceros sobre este usuario[131].

En las condiciones de uso de Facebook encontramos lo siguiente: "Es posible que Facebook utilice información de tu perfil sin identificarte individualmente ante terceros. Esto se hace con propósitos como establecer a cuanta gente en una red le gusta una película, y para personalizar anuncios y promociones".

El Informe de la Agencia Española de Protección de Datos referido a publicidad plantea como peligros el spam o social spammer, la publicidad hipercontextualizada y la instalación y uso de cookies sin el conocimiento de los usuarios.

En primer lugar, no debemos olvidar que es necesario el consentimiento del usuario para que se puedan utilizar los datos personales. Las redes sociales tratan de obtenerlo con la aceptación de las condiciones generales, lo cual es un tema dudoso.

Pero, además, Facebook declara que: "…almacenamos cierta información de tu navegador usando cookies… Podemos utilizar información sobre ti que recopilemos en otras fuentes incluyendo, entre otras, periódicos y fuentes de Internet como blogs, servicios de mensajería instantánea, la plataforma de desarrolladores de Facebook y otros usuarios de Facebook, para complementar tu perfil".

La principal cuestión que nos atañe es la utilización de cookies, sin olvidarnos de la vía de obtención del consentimiento y la recopilación de datos obtenidas de otras fuentes.

El Grupo de Trabajo del Artículo 29 en el Dictamen 1/2009 entiende que la configuración predeterminada del navegador, con carácter general, no puede entenderse como autorización previa para la obtención de datos personales. Por otra parte, la AEPD ha manifestado que Internet no es una fuente accesible

[131] PANIZA FULLANA, Antonia. "Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores". Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009. Página 47.

al público, por lo tanto será necesario obtener el consentimiento e informar previamente sobre la finalidad del tratamiento.

Relacionado al uso de datos por terceros y la cesión de datos, surge de las cláusulas de las redes sociales, por ejemplo en Facebook encontramos: "Los anuncios que aparecen en Facebook en ocasiones son enviados (o "servidos") directamente a los usuarios por anunciantes externos. Cuando esto ocurre, reciben automáticamente tu dirección IP. Estos anunciantes también pueden descargar cookies en tu ordenador o utilizar otras tecnologías como JavaScript e insignias de páginas web (también conocidos como "gifs 1x1") para medir la efectividad de sus anuncios y personalizar el contenido publicitario. Hacer esto permite a la red publicitaria reconocer tu ordenador cada vez que te envían un anuncio con el fin de medir la efectividad de su publicidad y personalizar el contenido. De esta forma, pueden recopilar información sobre el lugar donde las personas que utilizan tu ordenador o explorador han visto sus anuncios y determinar en qué anuncios hacen clic. Facebook no tiene acceso ni control de las cookies que puedan ser instaladas por estos anunciantes. Los anunciantes no tienen información de contacto almacenada en Facebook, excepto si decides compartirla con ellos[132].

Esta cláusula permite el uso de *web bugs*, que son pequeñas imágenes incluidas en las páginas web, pero pueden ser de un píxel transparente, por lo que pasan totalmente desapercibidos, y permiten la obtención de estadísticas sobre las visitas a los sitios web, crean un perfil del usuario y comunican información desde el sitio web a la empresa de marketing.

Pero no solo las cookies y los web bugs captan información de los usuarios. Las tecnologías de computación ubicua poseen el potencial de proporcionar unos niveles anteriormente inconcebibles de apoyo a las actividades humanas en distintos aspectos de la vida mediante sistemas que funcionan de forma discreta, basándose en tecnología invisible incorporada en entornos y artefactos del día a día. La computación ubicua se ha denominado también persuasive computing o calm computing, inteligencia ambiental, ordenadores de vestir y también Internet de las cosas, que se utilizan como sinónimos, si bien se centran en diferentes aspectos[133].

A su vez, una noticia reciente comenta que Facebook utilizaba cookies de conducta después que el usuario realizaba el logging de la red social.

[132] PANIZA FULLANA Antonia. "Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores". Ob. Cit. Página 55.
[133] CAS, Johann. "Computación ubicua, privacidad y protección de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes". Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009. Página 69.

Después de negar las acusaciones de que se puede rastrear lo que el usuario está haciendo en línea, incluso si se desconecta de la red social, Facebook ha cambiado la forma de comportarse de sus cookies. El fin de semana, el autoproclamado hacker de Nik Cubrilovic acusó a Facebook de seguimiento de sus usuarios, incluso si la sesión de la red social había finalizado. La compañía respondió negando las demandas y ofreció una explicación de por qué sus cookies se comportan de la manera que lo hacen. Ahora, dice Cubrilovic Facebook ha hecho cambios en el proceso de cierre de sesión, y detalló lo que cada cookie es responsable. Facebook cuenta con cinco cookies que persisten: datr, lu, p, L, y actuar. También hay dos cookies de sesión que persisten después de la desconexión procedimiento: a_user y a_xs. El primero, que es el identificador del usuario, ahora es destruido al salir. Así es como Facebook lo describe así: Lo que se ve en su navegador es en gran medida típica, excepto a_user que es menos común y debe ser limpiado al cierre de sesión (que se encuentra en algunas páginas de carga de fotos). Hay un error en el a_user no se ha borrado al cerrar la sesión. Vamos a fijar que en la actualidad la cookie datr se establece cuando un navegador visita primero facebook.com (excepto a través de plug-in iframes social), y ayuda a Facebook "identificar la actividad de inicio de sesión sospechosas y mantener a los usuarios a salvo." La cookie lu también se establece la primera vez que un navegador visita facebook.com y se utiliza para identificar el navegador, que ayuda a la cookie, es una cadena a_xs y se utiliza para prevenir ataques *cross-site scripting* "proteger a las personas que usan computadoras de uso público", que sirve para comprobar la capacidad de carga de las peticiones al servidor. Estas cookies identifican el navegador utilizado, incluso después de cerrar la sesión, y Cubrilovic dice que no debe preocuparse por ellos, a menos que usted no crea que Facebook utiliza dichas cookies con la finalidad que se describe. Cubrilovic dice que el resto de las cookies no son muy interesantes: "se pusieron las cosas como el idioma de su navegador y dimensiones del dispositivo". Él cree que la cookie más interesante, a_user, ahora se comporta como debería[134].

También referido a Facebook, me interesa compartir la nota de prensa, porque tiene connotaciones diferentes, ya que enfoca la publicidad desde la perspectiva del usuario de la red social y dice que: El Marketing digital ha mostrado un crecimiento vigoroso durante los primeros meses del 2011, especialmente en el marketing en motores de búsqueda, el que creció un 17%. La publicidad en Facebook también se ha ido tornando más competitiva, con un aumento del 40% en el costo por clic y una gran demanda por productos publicitarios. En los últimos trimestres se ha visto un gran impulso a la publicidad de Facebook y los anunciantes están ansiosos por aprovechar todas las capacidades que ofrece su mercado para interactuar con fans y promocionar sus marcas. Por esto, el costo por clic de Facebook ha crecido y cada día es

[134] PROTANLINSKI, Emil. "Facebook fixes cookie behavior after logging out". http://www.zdnet.com/blog/facebook/facebook-fixes-cookie-behavior-after-logging-out/4120 Página visitada 4 de octubre de 2011.

más competitivo, estimándose que los ingresos de Facebook se doblarán este año, alcanzando así los 4.000 millones de dólares. La gran red social será sin duda, el péndulo que determinará el precio de la publicidad online. Los anunciantes han apostado por este nuevo medio publicitario y el entorno se vuelve cada vez más competitivo, estando dispuestos a pagar más para llegar al consumidor. No es de extrañar en este caso, que Facebook tenga como principal fuente de ingresos la publicidad[135].

## 4. DICTAMEN 2/2010 DE 22 DE JUNIO DE 2010 SOBRE PUBLICIDAD COMPORTAMENTAL EN LINEA

El dictamen de referencia está fechado el 22 de junio de 2010, teniendo plazo los Estados miembros de la Unión Europea hasta mayo de 2011 para incorporar la Directiva 2009/136/CE.

El Dictamen analiza cuales son las funciones y las responsabilidades de los distintos actores involucrados en la publicidad comportamental y determina:

a) En relación a los Proveedores de redes de publicidad: en publicidad comportamental la obligación de obtener el consentimiento informado corresponde a los proveedores de redes de publicidad.

Por otra parte, estos proveedores desempeñan el papel de responsables de tratamiento de datos, ya que tienen un control completo de los objetivos y medios del tratamiento de datos.

b) En relación a los Editores: ceden espacio en alquiler en sus sitios a las redes de publicidad para colocar anuncios y configuran sus sitios de modo que los buscadores de los visitantes sean redireccionados automáticamente a la página del proveedor de redes de publicidad, que le enviará la cookie y publicidad a medida.

El Grupo de Trabajo del Artículo 29 entiende que los editores tienen cierta responsabilidad en el tratamiento de datos porque con la configuración del sitio *desencadenan* la transferencia de la dirección IP. Pero como éstos no retienen información personal, no tiene sentido aplicarles disposiciones como por ejemplo el derecho de acceso. Pero no cabe dudas que tienen la obligación de informar a las personas sobre el tratamiento de datos.

[135] GUNCKEL, Tony. Vicerrector Universidad Tecnológica de Chile INACAP. Sede Rancagua. http://eltipografo.cl/2011/04/facebook-y-el-marketing-digital-en-el-2011/ Página visitada el 20 de abril de 2011.

Junto con los proveedores de redes de publicidad, los editores “deben garantizar que la complejidad y las características técnicas del sistema de publicidad orientada por el comportamiento no les impidan encontrar las vías adecuadas para cumplir con las obligaciones que incumben a los responsables del tratamiento y salvaguardar los derechos de los interesados”[136].

Los acuerdos de servicios entre editores y proveedores de redes de publicidad deben establecer las funciones y responsabilidades de ambas partes de acuerdo con el tipo de colaboración que se describa en los mismos.

c) En relación a los anunciantes, establece el Dictamen que: “si el anunciante capta información de rastreo (por ejemplo determinados datos demográficos como “madres jóvenes” o un grupo de interés como “aficionado al deporte de riesgo”) y lo combina con los datos del comportamiento del usuario al navegar o sus datos de registro, puede decirse que el anunciante es responsable del tratamiento de datos independiente en esa fase del tratamiento”.

Sobre estos aspectos, explica Allan Pannetrat[137] que hay intermediarios fundamentales entre los anunciantes que desean promocionar un producto y los editores que buscan ingresos por venta de espacio para mostrar anuncios. Esto funciona con la tecnología "cookies", en la mayoría de los casos las cookies de terceros. Es decir, las cookies no proceden de la editorial que está mostrando el contenido principal del sitio web, sino de la tercera parte, que es la red de publicidad.

Aunque no se conozca su nombre y su dirección, es considerado por nosotros datos personales en la medida en que se puede seguir a la persona e individualizarla.

La presente Directiva se aplica independientemente del hecho de que las cookies se consideren o no datos personales. Me gustaría destacar – dice Pannetrat- que, la Directiva 2002/58/CE tiene prioridad sobre la Directiva de 95/46/CE en estas materias, porque es una directiva específica.

Tenemos básicamente dos tipos de cookies. Son las cookies que se necesitan para proporcionar el servicio solicitado específicamente por el usuario. Podemos ver ejemplos de esto: su carro de la compra puede estar en una "cookie" cuando usted está comprando cosas en un sitio web en Internet, puede ser una cookie de sesión, cuando se conecta a su banco, una cookie a veces de preferencia. Para este tipo de cookies que no tienen una pregunta de opt in o opt out o consentimiento en la mayoría de los casos.

[136] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 1/2010 de 16 de febrero de 2010 sobre los conceptos de “responsable del tratamiento” y “encargado del tratamiento”.
[137] PANNETRAT, Allan. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

Los otros tipos de cookies como OBA tienen un régimen específico. Básicamente se entiende que el almacenamiento o acceso a las cookies en el equipo terminal sólo está permitido a condición de que el abonado o usuario haya dado su consentimiento por haber recibido información clara y comprensible. Así que, cuando se rompe esto, el primer paso es la información, el segundo paso es el consentimiento y para el almacenamiento o no de la información en el terminal del usuario se requiere el consentimiento previo.

### 4.1 Obligación de obtener el consentimiento previo de los usuarios

El artículo 5 apartado 3 establece que un proveedor de redes de publicidad que desee almacenar información o tener acceso a información almacenada en el equipo terminal del usuario, puede hacerlo si:

a) ha proporcionado al usuario información clara y completa con arreglo a la Directiva 95/46/CE, especialmente sobre el objetivo del tratamiento de los datos;

b) ha obtenido el consentimiento del usuario para el almacenamiento o el acceso a la información en su equipo terminal, tras haberle proporcionado la información mencionada en el punto anterior.

Por tanto, el consentimiento debe ser previo e informado y por supuesto debe ser revocable.

Con relación al punto de si la configuración del buscador implica consentimiento, ya que se proporciona información en los términos y condiciones generales o usos de privacidad en relación a cookies de terceros utilizados para publicidad comportamental. Pero el Grupo de Trabajo del Artículo 29 entiende que esta práctica no cumple con el artículo 5 apartado 3, especialmente en la versión modificada, que hace hincapié en proporcionar información previa y obtener el previo consentimiento.

Se fundamenta en que el Considerando 66 de la Directiva 2002/58/CE 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*". Y aclara que esto no supone una excepción al artículo 5 apartado 3, sino un recordatorio de que en un entorno tecnológico el consentimiento puede darse de diferentes formas. Pero destaca a tener en cuenta que los usuarios normales no son conscientes del rastreo a que se somete su comportamiento en línea ni sus objetivos y muchas veces no saben configurar el buscador para rechazar las cookies. Por tanto, no es posible considerar que si el usuario no configuró su navegador para rechazar las cookies supone un consentimiento.

De acuerdo al Dictamen 2/2010 para que los buscadores u otras aplicaciones puedan ser indicativos de consentimiento válido deben:

a) Por defecto, rechazar cookies de terceros y requerir que el usuario realice una acción expresa para aceptar la configuración de una transmisión continuada de información contenida en los cookies por sitios web específicos.

b) Los buscadores, juntos o en combinación con otras herramientas de información, deben transmitir información clara, completa y perfectamente visible para garantizar que el consentimiento esté plenamente fundamentado. Las advertencias genéricas, sin referencia explícita a la red de publicidad que está instalando el cookie, no son suficientes.

Los proveedores de redes de publicidad ofrecen sistemas de exclusión voluntaria que permitan a los usuarios optar por no recibir publicidad a medida. Tales sistemas no son adecuados para obtener el consentimiento de un usuario corriente, si bien son positivos en la medida que facilitan la exclusión voluntaria.

Ya la Recomendación 1/1999 sobre tratamiento invisible y automático de datos personales en Internet establecía: “En el caso de cookies, debería informarse al usuario cuándo está previsto que el software de internet reciba, almacene o envíe un cookie. El mensaje debería especificar, en un lenguaje normalmente comprensible, qué información se pretende almacenar en el cookie y con qué objetivo así como el período de validez del cookie”.

Cuando el considerando 25 de la Directiva 2002/58/CE dice que: “*el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión… en conexiones posteriores*”, puede entenderse que si la persona acepta una cookie no solo acepta el envío sino también la ulterior recogida de datos.

En este sentido el Grupo de Trabajo del Artículo 29 entiende que la aceptación no puede ser de una vez y para siempre y propone tres líneas de acción:

1. limitar el alcance del consentimiento en el tiempo,

2. se debe dar información complementaria y

3. el consentimiento dado siempre puede revocarse.

Respecto al consentimiento de los niños, el Grupo de Trabajo del Artículo 29 estima que los proveedores de redes de publicidad no deben ofrecer grupos de interés dirigidos a enviar publicidad comportamental a los niños o influir en ellos.

Es relevante tener en cuenta en este punto la Opinión 15/2011 del Grupo de Trabajo del Artículo 29 de 13 de julio de 2011 sobre la definición de consentimiento.

El dictamen hace un análisis exhaustivo del concepto de consentimiento como se utilizan actualmente en la Directiva de Protección de Datos y en la Directiva sobre la privacidad. Basándose en la experiencia de los miembros del Grupo de Trabajo del artículo 29, el dictamen ofrece numerosas ejemplos de un consentimiento válido y no válido, centrándose en sus elementos clave, tales como el significado de "indicación", "libremente", "específico", "sin ambigüedades", "explícito", "informada", etc. El dictamen, además, aclara algunos aspectos relacionados con la noción de consentimiento. Por ejemplo, el momento de cuándo debe obtener el consentimiento, como el derecho a oponerse difiere de consentimiento, etc.

El dictamen se emitió en parte en respuesta a una petición de la Comisión en el contexto de la actual revisión de la Directiva de Protección de Datos. Por lo tanto, contiene recomendaciones para su consideración en la revisión. Esas recomendaciones incluyen:

i. aclarar el significado de "sin ambigüedades" el consentimiento y explicar que el consentimiento sólo que se basa en las declaraciones o acciones para expresar acuerdo constituye un consentimiento válido;

ii. tratamiento de los datos que requieren para poner en marcha mecanismos para demostrar el consentimiento;

iii. la adición de un requisito explícito en relación con la calidad y accesibilidad de la información que constituye la base para el consentimiento, y

iv. una serie de sugerencias con respecto a los menores y demás incapaces.

El Dictamen refiere a lo establecido en los artículos 6 (3), 9, 13 y 5 (3) respecto al tiempo que se requiera el consentimiento. Diversas disposiciones de la Directiva sobre la privacidad contienen un lenguaje explícito o implícito lo que indica que el consentimiento debe ser siempre previo al tratamiento. Esto está en consonancia con la Directiva 95/46/CE.

El artículo 6 (3) de la Directiva sobre la privacidad incluye una referencia explícita al consentimiento previo del abonado o usuario afectado, se establece la obligación de proporcionar información y obtener el consentimiento previo antes de procesar datos de tráfico con fines de venta servicios de comunicaciones electrónicas o servicios de valor añadido. Para ciertos tipos de

servicios, el consentimiento puede ser obtenido por parte del abonado en el momento de la suscripción de los de servicio. En otros casos, puede ser viable obtenerlo directamente del usuario.

Un enfoque similar al adoptado en virtud del artículo 9 sobre el tratamiento de datos de localización aparte de los datos de tráfico. El proveedor del servicio deberá informar a los usuarios o abonados - antes de la obtener su consentimiento el tipo de datos de localización aparte de los datos de tráfico que serán procesados. El artículo 13 establece el requisito de obtener el consentimiento previo de los usuarios pudiendo utilizar los sistemas automáticos de llamada sin intervención humana, fax o email con fines de venta directa.

Un ejemplo de esto se puede encontrar en el artículo 5 (3) de la antigua Directiva sobre privacidad, que dice (énfasis añadido): "el uso de redes de comunicaciones electrónicas para almacenar información o para obtener acceso a la información almacenada en el equipo terminal de un abonado o usuario sólo está permitido a condición de que el abonado o usuario tenga información clara y completa de acuerdo con la Directiva 95/46/CE, en particular sobre los fines del tratamiento, y se ofrece el derecho a negarse a dicho tratamiento por el responsable del tratamiento. "Esto debe compararse con la nueva redacción del artículo 5 (3) de la Directiva sobre la privacidad en su versión modificada por la Directiva 2009/136/EC, que establece que "(...) *el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario sólo está permitido a condición de que el suscriptor o usuario haya dado su consentimiento* (...)". Las consecuencias de este cambio en la redacción del artículo 5 (3) han sido explicadas por el Grupo de Trabajo del Artículo 29 en su Dictamen 2/2010 sobre la publicidad comportamiento en línea.

Respecto al artículo 13 (2-3), derecho de oposición y su distinción de consentimiento se establece que: "...*los clientes de manera clara y muy clara se les da la oportunidad de oponerse...*".

En cuanto a la utilización de aparatos de llamada automática, máquinas de fax y correo electrónico, se requiere el consentimiento previo del interesado.

Si el destinatario de la comunicación comercial es un cliente existente y la comunicación tiene como objetivo la promoción de productos similares o propios del proveedor o servicios, el requisito no es el consentimiento, sino asegurar que a las personas "se les da la oportunidad de objetar" ex artículo 13 (2). El Considerando 41 explica el razonamiento de por qué el legislador, en este caso, no requería el consentimiento: "*En el contexto de una relación con los clientes existente, es razonable admitir el uso de los contactos electrónicos para la oferta de similares productos o servicios*". Así, en principio, la relación contractual entre él y el proveedor de servicios es la base legal que permite el

primer contacto por correo electrónico. Sin embargo, las personas deben tener la oportunidad de oponerse a nuevos contactos. Como el Grupo de Trabajo ya ha indicado: "Esta oportunidad debe seguir ofreciéndose con cada mensaje de marketing directo posterior, sin cargo alguno, con la excepción de los costos de la transmisión de esta negativa".

La necesidad del consentimiento debe ser distinguido de este derecho de oposición. El consentimiento basado en la falta de acción de los individuos, por ejemplo, a través de los casilleros ya marcados, no cumple con los requisitos de consentimiento válido en virtud de la Directiva 95/46/CE.

La misma conclusión se aplica a la configuración del navegador que acepta por defecto, la orientación de los usuarios (a través del uso de cookies). Esto es claro en la nueva redacción del artículo 5 (3).

Estos dos ejemplos no cumplen, en particular, los requisitos para una indicación inequívoca de deseos. Es indispensable que al interesado se le dé la oportunidad de tomar una decisión y para expresarlo, por ejemplo, marcando la casilla de sí mismo, teniendo en cuenta el propósito del procesamiento de datos.

En su dictamen sobre la publicidad comportamental el Grupo de Trabajo ha concluido que "parece de suma importancia que a los navegadores se los provea de configuración de protección de privacidad.

En otras palabras, de ser provistos de la configuración de "la no aceptación y no la transmisión de cookies de terceros". Como complemento de esto y para que sea más eficaz, los navegadores deberían exigir a los usuarios que atraviesen un asistente de privacidad cuando ellos instalan o actualizan el navegador por primera vez y proporcionar una manera fácil de ejercitar la elección durante el uso".

### 4.2 Obligación de información

En la publicidad comportamental los usuarios deben recibir información de la identidad del proveedor de la red de publicidad, del objetivo del tratamiento de sus datos, debe conocer que el cookie permitirá al proveedor conocer sus visitas a los diferentes sitios web, los anuncios en que en ha cliqueado, el tiempo que ha permanecido, etc.

El Considerando 25 de la Directiva 2002/58/CE establece que la información debe ser clara y precisa y estar tan asequible para el usuario como sea posible.

Quien tiene la obligación de proporcionar la información es quien envía y lee la cookie. Pero ya habíamos mencionado que los editores tienen la obligación de

informar a los usuarios sobre el tratamiento de sus datos al redireccionar su buscador. El Grupo de Trabajo del Artículo 29 no sugiere que se envíe información dos veces, sino que considera que en este campo hay una necesidad clara de cooperación entre los proveedores de publicidad y editores para decidir quién proporciona la información y como debe hacerlo.

James Mullock[138] destaca que la intención de la política de privacidad era explicar a los visitantes del sitio web, con toda claridad cómo su información se recopila y cómo se utilizarían. Con el tiempo, lo que se han convertido en una especie de mecanismo de defensa jurídica en las empresas para divulgar todos los posibles usos que podrían hacer de la información personal con el fin de tratar de protegerse de una demanda legal.

### 4.3 Otras obligaciones y principios derivados de la Directiva 95/46/CE

Cualquier categorización posible de los usuarios basada en datos sensibles implica que puedan cometerse abusos, por tanto los proveedores de redes de publicidad que ofrecen y utilicen categorías de interés que revelen información sensible, deben cumplir con el artículo 8 de la Directiva 95/46/CE.

Este artículo prohíbe el tratamiento de datos sensibles excepto en determinadas circunstancias específicas, que en este caso la única base jurídica para legitimar el tratamiento sería un consentimiento explícito y específico. Por tanto dicho consentimiento no puede obtenerse configurando el buscador.

El Grupo de Trabajo del Artículo 29 es consciente de que los perfiles reunidos y utilizados en publicidad comportamental podrían utilizarse para objetivos distintos de la publicidad, como por ejemplo para desarrollar nuevos servicios de índole aún no definida. Pero esto está condicionado al cumplimiento del artículo 6 apartado 1 letra b) que establece el principio de limitación de objetivos, que prohíbe el tratamiento de datos personales que no sean compatibles con los fines que hicieron legítima la recogida de datos inicial. Por tanto, la segunda utilización de información recogida y almacenada con fines de publicidad comportamental iría en contra del artículo 6 letra b) de la Directiva 95/46/CE.

Dice el Dictamen 2/2010 que: “Si los proveedores de redes de publicidad desean utilizar la información reunida con fines de publicidad comportamental para fines segundos e incompatibles, por ejemplo en otros servicios, necesitan una nueva base de datos jurídica para ello con arreglo al artículo 7 de la Directiva 95/46/CE. Por ello, deberán informar a los usuarios y, en la mayoría de los casos, obtener su consentimiento con arreglo al artículo 7 letra a)”.

[138] MULLOCK, James. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

Pero además, el artículo 6 apartado 1 letra e) dispone la eliminación de los datos cuando dejen de ser necesarios para los fines recogidos, es el principio de conservación de los datos. Por lo cual, la información sobre el comportamiento de los usuarios debe eliminarse si ya no es precisa para desarrollar un perfil. Y establece el dictamen que: "Todo responsable de tratamiento de datos debe poder justificar la necesidad de un período de conservación determinado".

También deben cumplirse los derechos de acceso, rectificación, eliminación y oposición. El Grupo de Trabajo del Artículo 29 conoce iniciativas de proveedores de redes de publicidad por las que se ofrece acceso a categorías de interés con las que se etiqueta a las personas en base al número ID del cookie, para que las personas puedan modificarlas o eliminarlas.

Los proveedores de redes de publicidad también deben garantizar el cumplimiento de las disposiciones de transferencias de datos personales a países terceros, por ejemplo cuando los servidores están situados fuera de la Unión Europea.

Mullock[139] considera que existen otras áreas a considerar, vemos varias capas de protección de datos, antes de entrar en las "cookies" propiamente dichas, como es la problemática de las direcciones IP, el conocimiento y consentimiento y toda la cuestión referente al opt in y opt out. Los casos que han pasado por los tribunales aquí en este momento tienden a su vez en sus hechos que ha habido un caso reciente en Suiza que se encuentra que las direcciones IP son datos personales. Pero, si las direcciones IP son datos personales, entonces usted realmente necesidad ver el estilo de la OBA que está teniendo lugar y los detalles de la operación especial de entender si se podría aplicar la ley de privacidad para su funcionamiento en virtud de los datos personales tratados.

El segundo punto es la piedra angular de la Directiva sobre protección de datos, es el concepto de conocimiento y consentimiento, y, en particular, el concepto de consentimiento libre e informado plenamente. Así que la idea de que opt in opt out en relación a las cookies es el final de la historia, sería muy miope.

El tercer punto refiere a toda la cuestión de opt in opt out que no es aplicable sólo a las cookies. Como parte de la directiva PEC es muy aplicable en relación con otras formas de comercialización o el canal de comercialización. Es muy importante para, por ejemplo, el uso de los datos de tráfico y de localización.

Con relación a las opiniones que ha generado el Dictamen, me ha parecido interesante aportar las reflexiones que ha generado.

[139] PANNETRAT, Allan. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

En ese sentido, Kimon Zorba[140] se pregunta acerca de su posición sobre el Dictamen del Grupo de Trabajo del Artículo 29. Y responde: nosotros en realidad damos una gran bienvenida a que la posibilidad de discutir el tema. Creo que nos merecemos una primera discusión sobre el propio dictamen y la forma en que lo vemos es muy importante porque tenemos aquí un público principalmente de América (se refiere a la Conferencia citada). Lo vemos como un aporte muy interesante, algunas de las cuestiones planteadas son muy válidas, otras con las que probablemente estemos firmemente en desacuerdo. No hemos visto ninguna prueba y hemos preguntado, y en la revisión legislativa de la directiva aprobada no se presentó prueba alguna de que OBA cause cualquier problema grande. La gente está preocupada sobre todo tipo de cosas y no negamos que pueda haber problemas, y pensamos que también hay algunas preocupaciones legítimas con OBA. Sin embargo, no hemos visto ninguna evidencia de que este es un problema real en el mercado.

Su principal crítica al Dictamen del Grupo de Trabajo del Artículo 29 es que “no ha sido muy conciso y preciso el trabajo en la argumentación jurídica de por qué en el artículo 5 (3) "antes" significa consentimiento expreso. Cree que esta es una de las principales deficiencias de la opinión y merece ser considerado en más detalle. (…) Lo que se establece en los considerandos en realidad no es jurídicamente vinculante. Así que, cuando los Estados miembros implementen la Directiva pueden prescindir totalmente de los considerandos. Por otra parte vemos en el Dictamen del Artículo 29 cosas que tendrían que ser una nueva forma de configuración del navegador y esto es un poquito difícil. Tengamos en cuenta que las cookies son las cookies. No hay ninguna diferencia real, la diferencia que creamos es puramente jurídica. Si lo desea, puede colocar una cookie de terceros y hacer que se vea como una cookie de primera parte. Todo eso posible. Creo que, haciendo tales distinciones y tratando de manera diferente, legalmente puede ser probablemente desafiante. La Directiva no habla acerca de las cookies, se trata de software, con más precisión, es acerca de las tecnologías de almacenamiento. Por lo tanto, todas las tecnologías de almacenamiento como HTML5, al igual que muchos de los productos de Adobe que almacenan la información local en un PC será capturado por la presente Directiva. Creo que es mucho más grave que simplemente hablar acerca de las cookies. Pero actualmente, creo que la atención se centra en las cookies”.

[140] ZORBA, Kimon. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

## 5. Dictamen 4/2012 sobre la excepción del consentimiento para las cookies

Como hemos analizado en el punto 4.1 el Artículo 5.3 de la Directiva 2002/58/CE, modificado por la Directiva 2009/136/CE, establecía el requisito del Consentimiento Informado, antes de que los datos fueran tratados en el equipo del usuario.

En virtud de ese artículo, se establecía la exención del consentimiento informado al cumplirse alguno de estos dos criterios:

> A. Cuando la cookie sea utilizada con el único propósito de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas.
>
> B. Cuando la cookie resulte estrictamente necesaria para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

El reciente Dictamen 04/2012 de 7 de junio del presente analiza estos dos requisitos a los efectos de determinar si una cookie está exenta o no del consentimiento informado, aclarando que el análisis se lleva a cabo sin perjuicio del derecho a ser informado y el derecho a oponerse establecido por la Directiva 95/46/CE, que se aplican a tratamiento de datos personales con carácter general.

En el Criterio A deben considerarse al menos tres elementos como estrictamente necesarios para que exista una red de comunicaciones entre dos partes:

1) La capacidad para dirigir la información a través de la red, en particular mediante la identificación de los extremos de la comunicación.

2) La capacidad de intercambiar los elementos de los datos en el orden previsto, en particular mediante la numeración de los paquetes de datos.

3) La capacidad de detectar errores de transmisión o pérdida de datos.

Con relación al Criterio B tiene que pasar las dos siguientes pruebas:

1) El servicio de la sociedad de la información ha sido expresamente solicitado por el usuario: el usuario (o suscriptor) hizo una acción positiva para solicitar un servicio con un perímetro claramente definido.

2) La cookie es estrictamente necesaria para habilitar el servicio de sociedad de la información: si las cookies están deshabilitadas el servicio no funcionará.

El dictamen retoma la clasificación de las cookies en: cookies de sesión o cookies persistentes, de primeras o terceras partes. Luego del análisis de las características de una cookie y de los diferentes escenarios posibles, concluye que las siguientes cookies pueden estar exentas de la obligación del consentimiento informado, bajo determinadas condiciones y siempre que no sean utilizadas para otros fines.

1. "*User input cookies*" (*cookies* de sesión utilizadas típicamente cuando el usuario ingresa a un sitio), son temporales y se eliminan al finalizar la sesión. Estas cookies son necesarias para prestar un servicio en Internet y además el usuario solicita el servicio y realiza una acción, como hacer clic en un botón o completar un formulario.

2. *Cookies* de autenticación: se utilizan para la autenticación del usuario en un sitio web, para ver información de su cuenta, saldo o transacciones. Funcionan únicamente mientras dura la sesión y puede aplicárseles el criterio B, el cual no se aplica cuando se trate de cookies persistentes.

3. *Cookies* de seguridad, utilizadas para prevenir abusos en la autenticación, como por ejemplo, detectar repetidos intentos fallidos de validación, siempre que tengan una duración limitada y no se refiera a servicios no solicitados por el usuario.

4. *Cookies* de sesión de contenido multimedia, contienen datos técnicos de la sesión para reproducir video o audio, son conocidas como “flash cookies”, usadas por ejemplo Adobe Flash y expiran cuando finaliza la sesión.

5. *Cookies* de sesión de balanceo de carga, mientras dure la sesión. El balanceo de carga es una técnica que permite la distribución de la tramitación de las solicitudes del servidor web sobre un conjunto de máquinas a los efectos de optimizar el rendimiento. Esto puede realizarse con una cookie de sesión, que está exceptuada por el criterio A.

6. *Cookies* para la personalización de la interface - *"UI customization cookies".* Se utilizan por ejemplo para seleccionar el idioma del usuario, para recordar sus búsquedas, son de duración determinada y no pueden estar enlazadas con cookies persistentes como el nombre de usuario. Están exoneradas en base al criterio B.

7. *Cookies* de *plug-in* para compartir contenidos en redes sociales - "*Social plug-in content shared cookies*" identifican a los miembros de una determinada red social, siempre y cuando el usuario no haya realizado un "*log-out*" de la red social. Muchas de las redes sociales proponen "plug-in de módulos sociales" que los operadores de sitios web pueden integrar en su plataforma, en particular para permitir a los usuarios de redes sociales compartir contenidos que les gustan con su "Amigos" y proponer otras funcionalidades relacionadas como la publicación de comentarios. Entiende el Grupo de Trabajo del Artículo 29 que las redes sociales que desean utilizar cookies con fines adicionales ( o una vida útil más larga), más allá del criterio B tienen que informar y obtener el consentimiento.

El primer aspecto importante a tener en cuenta es la finalidad de la instalación de la cookie para determinar si está exenta o no del consentimiento y siempre se necesitará éste cuando se trate de cookies de terceros. El segundo aspecto consiste en analizar que es estrictamente necesario desde el punto de vista del usuario, nunca del proveedor de servicios.

También se analizan en el Dictamen los casos de cookies que no están exceptuadas de obtener el consentimiento y son los siguientes:

1. "*Social plug-in tracking cookies*". Como se describió anteriormente, muchas de las redes sociales proponen "plug-in de módulos sociales" que en el sitio web los propietarios pueden integrar en su plataforma, para ofrecer algunos servicios que pueden ser considerados como "Solicitado expresamente" por sus miembros. Sin embargo, estos módulos también se puede utilizar para rastrear personas, tanto miembros como no miembros, como las cookies de terceros utilizadas para otros fines como por ejemplo la publicidad de comportamiento, análisis o estudios de mercado. Con esos fines, estas cookies no pueden ser consideradas "estrictamente necesarias" para proporcionar una funcionalidad expresamente solicitado por el usuario, por tanto no es posible aplicar el criterio B.

2. "*Third party advertising*". Las cookies de terceros utilizadas para la publicidad de comportamiento no están exentas de consentimiento como ya fue señalado en detalle por el Grupo de Trabajo en el Dictamen 2/2010 y en el Dictamen 16/2011. El requisito del consentimiento se extiende a todas las cookies de terceros relacionadas con el funcionamiento utilizado en la publicidad, incluyendo cookies utilizadas con el propósito de limitación de frecuencia, detección de fraudes, investigación y análisis de mercado, mejora y depuración del producto, ya que ninguno de estos fines se puede considerar que estar relacionado con un servicio o funcionalidad de un servicio de la sociedad de la

información expresamente solicitado por el usuario, como requerido por el criterio B.

El Grupo de Trabajo ha participado activamente desde el 22 diciembre de 2011 en la labor de la World Wide Web Consortium (W3C) para estandarizar la tecnología y el significado del no rastreo. En vista del hecho de que las cookies a menudo contienen identificadores únicos, que permiten el seguimiento del comportamiento del usuario a través del tiempo y a través de sitios web y la posible combinación de estos identificadores con otros datos de identificación, el Grupo de Trabajo está preocupado por la posible exclusión del no rastreo de determinadas cookies que se dice que son necesarios para fines operativos.

3. "*First party analytics*". Google Analytics es una herramienta de medición de estadística de audiencia de sitios web, que a menudo se basa en cookies. Estas herramientas son especialmente utilizadas por los propietarios de sitios web para estimar el número de visitantes únicos, para detectar las palabras clave de búsqueda más utilizadas del buscador que llevan a una página web o para localizar los temas de navegación web.

   Las herramientas de análisis disponibles en la actualidad utilizan una serie de datos diferentes, los modelos de recogida y análisis de cada uno de los cuales presentan diferentes riesgos para la protección de datos.

   También existen herramientas que utilizan cookies de "primer parte" con el análisis realizado por un tercero. Esta otra parte será considerada como un controlador común o como un procesador, dependiendo de si se utilizan los datos para sus propios fines o si está prohibido hacerlo a través de medidas técnicas o contractuales. Si bien se considera a menudo como una herramienta "estrictamente necesaria" para los operadores de sitios web, no son estrictamente necesarios para proporcionar una funcionalidad expresamente solicitada por el usuario.

El Dictamen finaliza estableciendo las pautas principales y concluye: "En última instancia, para decidir si una cookie está exenta del principio del consentimiento informado es importante verificar cuidadosamente si se cumple uno de los dos criterios de exención definidos en el artículo 5.3 de la Directiva 2009/136/CE. Después de un cuidadoso examen, si las dudas siguen existiendo respecto a si se aplica o no un criterio de excepción, los operadores de sitios web deberían examinar detenidamente si no existe en la práctica, la oportunidad de obtener el consentimiento de los usuarios de una manera discreta, sencilla, evitando así la inseguridad jurídica".

# CAPITULO V

# SITUACION ACTUAL

## 1. CODIGOS DE CONDUCTA Y SELLOS DE CALIDAD

Los Códigos de Conducta o Códigos de Prácticas Comerciales constituyen una forma de autorregulación. Estos códigos contienen las reglas que implican las mejores prácticas promulgadas por la industria, las asociaciones de comerciantes o las asociaciones de consumidores. Los códigos regulan el comportamiento de los proveedores y establecen normas de protección al consumidor[141].

Existe una multiplicidad de códigos establecidos por diferentes organismos. La mayoría ha tomado como modelo las Guías de la OCDE. Estos suelen utilizarse conjuntamente con los sellos de confianza.

Según María Jesús García "La decidida influencia del Derecho europeo en nuestro ordenamiento lleva a la aparición de crecientes fórmulas de autorregulación regulada. La LSSICE siguiendo la Directica de Comercio electrónico fomenta la autorregulación mediante códigos de conducta de los prestadores de servicios, predeterminando además aspectos de su elaboración, contenido, forma o accesibilidad (artículo 18 LSSICE). La propia previsión en dicha norma de un distintivo público de confianza constituye una manifestación más del fomento de la autorregulación en la Red[142].

Un sello de confianza funciona de la siguiente forma: es necesario que el proveedor se subscriba en forma voluntaria a un código de confianza, por el cual se compromete a respetar sus disposiciones y a pagar un precio por concepto de licencia, por lo cual se lo autoriza a utilizar el referido sello.

El sello de confianza en sí mismo es un símbolo o un logo que significa que el comerciante subscribió el código, que tiene como consecuencia proporcionar al proveedor una buena imagen comercial frente al consumidor.

A su vez, las empresas que proporcionan los sellos de confianza monitorean el cumplimiento del proveedor de dicho código y proporcionan un procedimiento para atender las quejas de los consumidores.

---

[141] DELPIAZZO, Carlos y VIEGA, María José. "Lecciones de Derecho Telemático. Tomo II". Lección 25. Ob. Cit. Página 134.

[142] GARCIA MORALES, María Jesús. "Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza". Capítulo del libro Consumidores y usuarios ante las nuevas tecnologías. Lorenzo Cotino Hueso (coordinador). Derecho y tic's. Valencia, 2008. Página 280.

Existen sanciones en caso de incumplimiento del proveedor con lo estipulado en el código, siendo la mayor penalidad la cancelación de la licencia para utilizarlo, lo que implica una publicidad negativa para el mismo.

El establecimiento de un régimen de garantías para la protección de los datos personales -realmente de las personas titulares de dichos datos, concepto que a veces no se desprende claramente del término por el que conocemos la materia- es una verdadera historia de éxito europea, pues no en balde es la Unión Europea el lugar del mundo en el que se otorga la máxima protección en este campo y se la considera un derecho fundamental de las personas. Sin embargo, hoy en día es obvio que la privacidad y la protección de datos personales no pueden basarse exclusivamente en regulaciones legales y en los mecanismos coercitivos que puedan ponerse en marcha para respaldar el cumplimiento de las mismas. Las constantes innovaciones en el campo de las TIC conducen a nuevas posibilidades de procesamiento de los datos personales -muchas veces de forma inadvertida o invisible para las personas- que necesitan de la aplicación de soluciones flexibles para que, sin perder las ventajas que la innovación tecnológica proporciona a la sociedad y a los ciudadanos, se garantice el respeto a la privacidad de las personas cuyos datos son objeto de tratamiento. Por lo tanto, el escenario actual obliga a encontrar nuevas aproximaciones a la protección de datos personales, no buscando nuevos derechos y principios, ya que ha quedado claramente demostrado que los existentes hasta la fecha proporcionan un marco de garantías adecuado, sino adaptando la forma en que estos principios y derechos se aplican en el actual entorno tecnológico, social, económico y político que es muy diferente del existente en los últimos años setenta y primeros noventa en los que la estructura básica del derecho fundamental a la protección de datos se estableció[143].

### 1.1 Código de Federación Europea de Marketing Directo e Interactivo (FEDMA)

La incidencia del marketing directo en la protección de datos personales ha sido motivo de intervención de la FEDMA (Federación Europea de Marketing Directo e Interactivo)[144]. Esta organización ha dictado un código de conducta para las empresas del sector, que fue sometido a la opinión del Grupo de Trabajo del Artículo 29 en dos oportunidades, lo que dio lugar al Dictamen 3/2003 relativo al Código de conducta europeo de la FEDMA sobre la utilización de datos

[143] ACED FÉLEZ. Subdirector General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM). “EUROPRISE: Certificados de Protección de Datos para Europa”. http://www.borrmart.es/articulo_redseguridad.php?id=1784 Página visitada 10 de octubre de 2011.
[144] http://www.fedma.org

personales en la comercialización directa (WP77) y Dictamen 4/2010 sobre el mismo tema, con referencia la comercialización en línea (WP174).

El Dictamen 4/2010 adoptado el 13 de julio de 2010 establece como presupuesto del documento el artículo 27 apartado 3 de la Directiva, referente a códigos comunitarios de conducta. El artículo establece: "*Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del Grupo contemplado en el artículo 29. Éste se pronunciará entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable al Grupo*".

El Anexo define una serie de términos aplicables en el sector, y trata diversos aspectos de la comercialización directa que requieren de la recogida y/o tratamiento de datos personales: envíos publicitarios, divulgación de listas, etc.

Se destacan:

- Definiciones.- Lista de definiciones incluyendo "comunicaciones comerciales no solicitadas", "tratamiento de datos personales" y "consentimiento", complementando las que ya estaban en el código general.

- Sección 2.- Requisitos para el tratamiento correcto de los datos, requisitos que debe cumplir el responsable, incluyendo disposiciones específicas sobre obtención de datos personales de consumidores y su comunicación a terceros. El correo electrónico publicitario debe incluir identificación clara del objeto, posibilidad al destinatario para darse de baja, y un método sencillo, efectivo y gratuito para no recibir más comunicaciones electrónicas, sin dar explicaciones.

- Sección 3.- Obtención de datos personales de fuentes distintas a la persona interesada. Expone requisitos para facilitar información a terceros por parte de responsable del tratamiento (consentimiento, reglas aplicables a campañas member-get-members).

- Sección 4.- Sistemas de servicios preferenciales.

- Sección 5.- Política de protección de datos personales y utilización de cookies. Al respecto el propio Dictamen sugiere la necesidad de ajustes en correspondencia con la Directiva 2002/58/CE modificada por la Directiva 2009/136/CE aplicable a partir del 25 de mayo de 2011.

- Sección 6.- Se da importancia a la protección de los menores en tanto sector especialmente vulnerable, como ya lo hacía el Código General de 2003. Especiales referencias sobre la ilicitud de solicitar datos sensibles a los menores, así como tratamiento de datos de salud, vida sexual o situación financiera de los mismos, terceros, padres o amigos.

- Sección 7.- Prácticas prohibidas.- Obtención automática de datos. "Programas espía". Remisión al ya citado Dictamen 2/2010 sobre Publicidad Comportamental en Línea.

Además, se incluye un anexo con ejemplos de mejores prácticas y prácticas no aceptables en la publicidad en línea, que ofrece un valor añadido para la aplicación práctica de las normas.

Finalmente, el Grupo de trabajo considera que el anexo sobre la comercialización en línea del "Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización "directa" es conforme a la Directiva 96/46/CE y a la Directiva 2002/58/CE aplicable actualmente, así como a la legislación nacional vigente. El Anexo aborda un buen número de temas importantes en el ámbito del sector de las actividades en línea (como las campañas *member-get-members*, la protección de los menores o la posibilidad de darse de baja) y, por tanto, proporciona el suficiente valor añadido a las Directivas al dar soluciones claras a las cuestiones planteadas en el sector de la comercialización en línea.

### 1.2 El Sello Europeo de Privacidad (EuroPriSe)

El Proyecto Sello Europeo de Privacidad (EuroPriSe) "establecerá un modelo de certificación para productos y servicios tecnológicos que cumplan con la normativa Europea de privacidad, protección de datos y seguridad. Esta certificación será realizada por autoridades independientes de certificación. El objetivo del proyecto EuroPriSe es establecer un procedimiento de certificación de aquellos productos y servicios tecnológicos que cumplan con la legislación Europea de privacidad, protección de datos y seguridad. Esta certificación se otorgará siguiendo un procedimiento dividido en dos fases: en primer lugar, una evaluación del producto o servicio a certificar, evaluación realizada por expertos jurídicos e informáticos. Realizada esta evaluación, estos expertos evacuan un informe que debe ser revisado por una entidad de certificación, para posteriormente, y siempre y cuando se cumpla con la normativa europea anteriormente citada, otorgar el Sello Europeo de Privacidad"[145].

Como hemos manifestado a lo largo del presente trabajo, uno de los problemas existentes en la sociedad de la información es la falta de confianza en los

[145] https://www.european-privacy-seal.eu/about-europrise/project-fact-sheet/fact-sheet-es.html

productos y servicios tecnológicos, que es necesario no solo para los usuarios, sino también para los empresarios.

El Sello de Privacidad se otorgará por una Agencia de Protección de Datos, una vez que un producto o servicio haya sido auditado. Esta auditoría deberá confirmar que es un producto o servicio "de confianza". De esta manera, el Sello de Privacidad, además de garantizar para los consumidores que dicho producto o servicio cumple con las normas europeas de privacidad, trata de ser una iniciativa para que los productores y vendedores ofrezcan garantías de cumplimiento de la privacidad en sus productos o servicios[146].

EuroPriSe trata de establecer:

- Un procedimiento voluntario de certificación válido en toda Europa.
- Un procedimiento transparente y basado en criterios fiables.
- La certificación por una autoridad independiente.
- Demostrar que la privacidad debe ser implementada en productos o servicios.
- La auditoría de productos o servicios tecnológicos a través de informes públicos.

EuroPriSe está dirigido a: productos y servicios tecnológicos cuya finalidad sea el almacenamiento de datos personales; a expertos jurídicos e informáticos y a Agencias de Protección de Datos que pueden actuar como Autoridades de Certificación.

El proyecto EuroPriSe está liderado por la Autoridad de Protección de Datos de la Región de Schleswig-Holstein (ICPP/ULD) de Alemania. Forman parte también de este proyecto la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), la Comisión Nacional de la Informática y la Libertad (CNIL), la Academia Austriaca de las Ciencias, la Universidad Metropolitana de Londres, y las empresas consultoras Borking (Holanda), Ernst and Young AB e (Suecia), TÜV (Alemania) y VaF (Eslovaquia).

"El sello se otorga en una ceremonia pública y tiene una validez de dos años, tras los cuales es necesario 're-certificar' el producto o servicio por si se hubieran producido cambios en el mismo que debieran ser revisados. Los productos aprobados pueden ostentar y mostrar públicamente el sello durante su periodo de validez. A la finalización del proyecto, se constituirá un Consejo

[146] https://www.european-privacy-seal.eu/about-europrise/project-fact-sheet/fact-sheet-es.html Página visitada 1 de octubre de 2011.

Europeo de Autoridades de Certificación encargado de supervisar que los procedimientos de certificación se aplican homogéneamente en todos los países y con un nivel de exigencia equivalente. EuroPriSe tiene una duración de dieciocho meses y acabará en diciembre de 2008. Durante el mismo se deben redactar informes técnicos y jurídicos y el catálogo de criterios y estándares que habrán de utilizarse pero, ante todo, como ya se ha indicado, se llevarán a cabo pruebas piloto en al menos seis países europeos -incluido España- para validar todo el procedimiento, comprobar su viabilidad y ajustar todos sus elementos. La Agencia de Protección de Datos de la Comunidad de Madrid, además de colaborar con el resto de socios en todas las actividades de EuroPriSe, está a cargo de este apartado fundamental: la evaluación de las pruebas piloto, definiendo su metodología y procesando los resultados que serán un elemento fundamental para preparar la versión final de los informes jurídicos y técnicos y, sobre todo, del Plan de Negocio para extender EuroPriSe a todos los países de la Unión Europea"[147].

El Sello de Privacidad Europeo certifica el cumplimiento de los productos y servicios de TI con la legislación comunitaria de protección de datos. Del comportamiento de sistemas de orientación, entre otros, están sujetos a la evaluación del sistema de certificación EuroPriSe. El rastreo del comportamiento de navegación del usuario en un sitio web o a través de varios sitios web se realiza por medio de cookies. El uso de cookies se rige por disposiciones específicas de la legislación de la UE sobre protección de datos. Como EuroPriSe se adhiere a la interpretación de la legislación comunitaria sobre protección de datos por el Grupo de Trabajo del Artículo 29, esta opinión será de gran importancia para el futuro de (re)certificación de los sistemas de búsqueda enfocado en el comportamiento, a través de un Sello Europeo de Privacidad[148].

El Sello de Privacidad Europea recientemente proporcionó orientación alrededor del marketing comportamental. Adopta el opt in, pero se logró a través de un sistema de iconos y acceso a los perfiles más recordatorios[149].

### 1.3 Alianza Europea por la Ética en la Publicidad (EASA) y Oficina de Publicidad por Internet (IAB)

[147] ACED FÉLEZ. Subdirector General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM). "EUROPRISE: Certificados de Protección de Datos para Europa". http://www.borrmart.es/articulo_redseguridad.php?id=1784 Página visitada 10 de octubre de 2011.

[148] "Position paper on the impact of the new "Cookie Law" on certifiability of behavioural advertising systems according to EuroPriSe". Julio 2010.

[149] ZORBA, Kimon. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

Fueron varias las noticias, bajo interesantes encabezados, que circularon en la web en torno a la preocupación de la adecuación de los distintos países a la llamada Directiva Cookies.

Se decía: Cuando la fecha límite para poner la Directiva en práctica fue mayo sólo Estonia, Dinamarca y el Reino Unido ha adoptado medidas para aplicarlo. Dinamarca ha decidido poner el proyecto de reglamento sobre el hielo por tiempo indefinido y el Reino Unido ha dado a las empresas un año para cumplir. La orientación sobre la ley de la Oficina del Comisionado de Información del Reino Unido es probablemente la más completa de cualquier Estado miembro hasta ahora. “Esta ley no puede cumplirse en cualquier forma razonable". El problema es la definición de "estrictamente necesario" es muy estrecha, dice Ben Allgrove, socio de la firma internacional de abogados Baker & McKenzie. "En los Países Bajos no hay discusión acerca de si el consentimiento debe ser "inequívoco ", que podría hacer que la configuración del navegador -una forma conveniente de obtener el consentimiento- es menos probable que sea aceptable", dice Matthew Norris, director mundial de tecnología y los medios de comunicación de la aseguradora Hiscox. "Comentaristas jurídicos alemanes y franceses usaron del término opt in por participar en el plazo y que es más draconiano que el Reino Unido, donde la Oficina del Comisionado de Información ha dicho específicamente que la legislación británica no constituye un requisito de opt in[150].

Este año (2011), el consenso parece ser la construcción en Bruselas para permitir que la industria de la publicidad en línea regule el uso de cookies. La principal industria del grupo es la Interactive Advertising Bureau de Europa, que creó un sitio Web para que los consumidores puedan optar por no recibir - "opt out" - publicidad dirigida, como resultado de los perfiles. El sitio es youronlinechoices.eu. Pero los reguladores que representan a los Estados miembros de la Unión Europea, apoyados por grupos de consumidores, están poniendo obstáculos al acuerdo voluntario, argumentando que no protegen adecuadamente a las personas, sin darse cuenta de que permite a los vendedores recoger datos personales[151].

El sitio web youronlinechoices.eu es de uso sencillo y permite que las personas opten por darse de alta o de baja de una lista de empresas que recogen y procesan información para realizar marketing comportamental.

En el sitio se recalca que hay que tener en cuenta que dar de baja los servicios de publicidad comportamental no significa que se dejará de recibir publicidad.

[150] MILLAR Michael. “Cookie: monster? How will business cope with new laws”. http://www.bbc.co.uk/news/business-13951107 . Página visitada el 7 de julio de 2011.

[151] O'BRIEN Kevin J. “Estableciendo límites de privacidad en Internet”. Publicado: 18 de septiembre 2011 http://www.nytimes.com/2011/09/19/technology/internet/setting-boundaries-for-internet-privacy.html?_r=3 Página visitada el 19 de setiembre de 2011.

Simplemente, la publicidad gráfica que va a visualizar en las páginas web que visita no será personalizada.

En el sitio se proporcionan cinco consejos claves[152] para ayudarle a gestionar su privacidad:

1. Seguridad y transparencia: los anunciantes no saben quien es usted, dado que la información se basa en su navegación pero no lo identifica.

2. Busque información sobre la publicidad comportamental en cualquier sitio web que visite. Las compañías informan quien recolecta la información, si es el propietario de un sitio web o de un tercero.

3. Forma de darse de baja.

4. Familiarícese con las opciones de privacidad de su navegador.

Frente a la adopción de la recomendación autorreguladora sobre mejores prácticas de publicidad comportamental en línea, el Grupo de Trabajo del Artículo 29 envió, en agosto de 2011, una carta abierta a la ENASA y el IAB en el que indicaba su preocupación por la protección de datos en el contexto del enfoque de exclusión voluntaria sugerido por el Código EASA/IAB.

En una reunión posterior con el Grupo de Trabajo del Artículo 29, los representantes de la EASA y el IAB señalaron que “la finalidad principal del Código es crear unas reglas de juego equitativas” y que su objetivo no era conseguir el cumplimiento de la Dirección revisada sobre privacidad en las comunicaciones electrónicas”[153].

El Grupo de Trabajo del Artículo 29 entiende que el Código EASA/IAB no resulta adecuado para garantizar el cumplimiento de lo dispuesto en el actual marco jurídico europeo, sobre protección de datos y analiza en el Dictamen 16/201 de 8 de diciembre de 2011 los principios en los que se basa dicho Código.

Principio del Aviso: para cumplir la legislación, el aviso, la información debe darse directamente al usuario en forma clara y previa a la recolección del dato. El Código lo soluciona mediante un ícono, que no se entiende apropiado en virtud del desconocimiento que tienen las personas respecto a la publicidad comportamental.

---

[152] http://www.youronlinechoices.com/es/cinco-consejos-clave/ Página visitada el 19 de setiembre de 2011.

[153] Comunicado de prensa del Grupo de Trabajo del Artículo 29 de 14 de setiembre de 2011: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

El segundo principio del código refiere a la elección sobre la publicidad comportamental en línea. El Código ofrece la posibilidad de oponerse, ya que permite darse de baja, lo que no cumple con el artículo 5 apartado 3 de la Directiva que hemos estudiado, porque no se cumple con el requisito del previo consentimiento informado.

De acuerdo al Dictamen "la primera aplicación práctica del código EASA/IAB es el sitio web www.yourinlinechoices.eu, donde el método seleccionado para "elegir" se basa en la utilización de diversas *cookies* "de autoexclusión". Gracias a este *cookie*, las redes publicitarias pueden registrar la negativa del usuario a seguir participando en la publicidad comportamental en línea. Este enfoque podría modificarse fácilmente de modo que se cumpliera el artículo 5, apartado 3, modificado de la Directiva, mediante la creación de un *cookie* de autoinclusión, como se explica más abajo".

La cookie de autoexclusión plantea los siguientes problemas:

a) Si bien impide la recepción de publicidad personalizada, no impide a la red publicitaria obtener y almacenar información en el terminal del usuario.

b) No se informa al usuario sobre si la cookie de seguimiento se mantiene o no almacenada en su ordenador ni su finalidad.

c) No ofrece la posibilidad de gestionar y borrar cookies de seguimiento instaladas previamente al tiempo que crea la presunción errónea de que la autoexclusión desactiva el seguimiento.

Además, el sitio contiene enlaces a funciones JavaScript que pueden recoger información como la dirección IP del usuario, su referenciador y la configuración personalizada de su navegador.

El Principio IV refiere a segmentación sensible, previendo una edad mínima de 12 años para el tratamiento de datos de menores, umbral que no tiene fundamentos jurídicos.

Con respecto a la exigencia de que los usuarios den su consentimiento expreso antes de crear o personalizar segmentos de publicidad comportamental en línea de datos personales sensibles, el GT29 la ha acogido con satisfacción.

Relativo al cumplimiento y aplicación previstos en el Principio VI, hay que tener en cuenta que el Código contiene medidas para asegurar que las empresas signatarias cumplan sus disposiciones, pero el GT29 observa que los reguladores nacionales son los responsables últimos de que los proveedores de PCL cumplan la ley y de aplicar las correspondientes medidas de ejecución.

Otro aspecto criticado en el Dictamen es que el Código no contiene disposiciones sobre la cantidad de datos recogidos y el período de conservación para fines específicos, tampoco el sitio web proporciona explicación sobre este tema.

La EASA y el IAB han alegado que la instalación de cada cookie exige consentimiento expreso y que esto incide negativamente en la navegación, motivo por el que el GT29 aclara en el Dictamen que no es necesario requerir el consentimiento para cada tipo de cookie, ya que existen diversas formas de usarlos, con distintos fines y requisitos. Y establece casos en que no es necesario el consentimiento: las cookies de acceso seguro, las utilizadas en las cestas de compra y las de seguridad. Este tema fue ampliado en el último Dictamen referido al tema, analizado anteriormente.

Otro punto que destaca el dictamen refiere a que el uso de una ventana desplegable no es la única forma de recibir el consentimiento. Y señala algunos ejemplos:

- Una banda informativa estática en la parte superior de los sitios web en la que se solicita el consentimiento del usuario para instalar algunas cookies, con un hiperenlace a una declaración de privacidad con una explicación detallada sobre los distintos controladores y los fines del tratamiento.

- Una pantalla introductoria en la que se explique, al entrar al sitio web, que cookies se instalarán y por parte de quien si el usuario da su consentimiento.

- Un ajuste de configuración por defecto que prohíba la transferencia de datos a terceros, que requiera al usuario pulsar un botón para indicar su consentimiento a fines de seguimiento.

- Un ajuste de configuración por defecto en los navegadores que permita evitar la recogida de datos comportamentales.

Tampoco es necesario pulsar en múltiples ventanas desplegables de consentimiento, como lo afirmaron la EASA y el IAB. Esta sugerencia no tiene en cuenta que una vez que se prestó el consentimiento no es necesario volver a solicitarse para instar otra cookie que tenga el mismo propósito y proceda del mismo proveedor.

## 2. PANORAMA COMPARADO DE LOS PAISES EUROPEOS

### 2.1 Alemania

Hasta ahora, se ha presentado al Parlamento un proyecto de ley del gobierno destinado a modificar la Ley de Telecomunicaciones alemana, que reconoce el riesgo de que las cookies se utilicen para crear perfiles de los usuarios, pero no indica la forma de aplicar el artículo 5 (3) de la Directiva. Sin embargo, antes de hacer alguna sugerencia de aplicación, el gobierno alemán quiere esperar para tener en cuenta los resultados de las consultas a nivel europeo que se están realizando.

Mientras tanto, en junio de 2011, el Bundesrat (Cámara Alta, donde los estados federales alemanes están representados) presentó el proyecto de ley (BR Dres. 156/11) con las enmiendas a la Ley Alemana de Telemedia (TMG), que entre otras cosas, contiene una disposición (artículo 13 párrafo 8 TMG) que requieren que los usuarios deban ser informados y requerido su consentimiento antes del almacenamiento de los datos en el dispositivo del consumidor final y/o cualquier acceso remoto a los datos. Este proyecto de disposición ha suscitado importantes críticas por ser demasiado amplio y no se considera para calificar como una implementación de la Directiva. El Gobierno considera realizar una enmienda a este proyecto relativo al tema cookies y presentarlo a TKG.

En agosto, sin embargo, el Gobierno federal alemán confirmó, como parte de una respuesta a una solicitud presentada por los miembros del Parlamento de fecha 3 de agosto 2011, (BT-Drs. 17/6765) que ahora tiene la intención de poner en práctica el artículo 5, párrafo 3 de la Directiva por la inserción del texto revisado en la mencionado enmienda del proyecto de la TKG.

Referido a  Alemania, se ha mencionado la existencia de la opinión de la DC. El DC es una asociación de reguladores de los Estados alemanes que regulan la protección de datos para el sector privado. Y hace un año lanzaron un dictamen en relación con Google Analytics y pidieron que opt in para crear perfiles de usuario para fines de análisis web. Muy inclinado hacia esta opción al final fue un dictamen de reglamentación, no la ley. Pero curiosamente, hace sólo hace un par de días, hicieron un comunicado de prensa en la que han dado su opinión de que Google Analytics sigue siendo ilegal. Esencialmente, se emitió un ultimátum a Google y se le dijo "usted tiene 8 semanas para mejorar y obtener el cumplimiento". De lo contrario, se comenzará a tomar medidas contra los editores que utilizan Google Analytics en Alemania[154].

[154] LEE, Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

En octubre de 2011, el Parlamento alemán (Bundestag) aprobó un proyecto de ley destinado a modificar la Ley de Telecomunicaciones (TKG).

De acuerdo con los motivos de la ley, el Bundestag reconoce el riesgo que implica el uso de las cookies para crear perfiles de un usuario, pero aún no se ha llegado a la forma de aplicar el artículo 5 (3) de la Directiva. El Bundesrat se opuso al proyecto y pidió al Comité de Conciliación (Vermittlungsausschuss), que espere hasta mayo de 2012.

## 2.2 Bélgica

No hay información sobre el tema en virtud a que el Consejo de Ministros aprobó un proyecto de texto de 1° de julio 2011, pero se espera que se envíe al Parlamento en octubre de 2011. Este documento no está accesible al público.

## 2.3 Dinamarca

La Ordenanza sobre los requisitos de información y el consentimiento para el almacenamiento o el acceso a la información en el equipo terminal del usuario final ha entrado en vigor el 14 de diciembre de 2011. Se puede encontrar información y orientación sobre las nuevas reglas, que incluyen lo referente a la utilización de cookies en Internet http://www.itst.dk/sikkerhed/privacy/lagring-af-og-adgang-tiloplysninger-PA-andres-udstyr

La Ordenanza tiene por objeto ayudar a proteger la privacidad de los usuarios cuando utilizan Internet. El aviso requiere información y consentimiento, entre otras cosas, los servicios digitales utilizan cookies y tecnologías similares, que se almacenan en los ordenadores de los usuarios, teléfonos inteligentes y otros equipos. El uso de cookies y tecnologías similares son ampliamente utilizados y pueden tener una variedad de propósitos, tales como la personalización y el desarrollo de la utilización más fácil de los servicios, la generación de análisis sobre el uso de un sitio web o dirigirse a la comercialización del comportamiento para los usuarios. La capacidad de los usuarios a decidir por sí mismos si van a ser identificados a través de cookies y tecnologías similares en su equipo terminal es un elemento esencial en la protección de su privacidad en un mundo cada vez más digital[155].

[155] http://www.itst.dk/sikkerhed/privacy/lagring-af-og-adgang-til-oplysninger-pa-andres-udstyr Página visitada el 28 de abril de 1012.

## 2.4 Eslovaquia

Hay un proyecto de legislación que se encuentra en el Parlamento en la segunda etapa.

Las normas para las cookies están reguladas en el artículo 55 (5) de la nueva ley de comunicaciones electrónicas N° 351/2011 Colll. No hay guías ni recomendaciones en lo que respecta a las cookies. Sin embargo la configuración del navegador ha sido publicada o puesta a disposición.

## 2.5 España

En términos generales, aunque el consentimiento a las cookies sea expresado a través de la configuración del navegador web requiere que el receptor lo configure activamente, realizando ajustes para dar su consentimiento durante la instalación o actualización. Esto va más allá de la redacción del Considerando 66 de la Directiva.

El gobierno publicó un proyecto de propuesta a consideración del Parlamento. El plazo para la modificación fue de 5 Julio de 2011 y varias enmiendas fueron propuestas. Los proyectos de propuestas son objeto de un informe de la Comisión de Industria del Parlamento.

El pasado 24 de mayo de 2011 se aprobó el Proyecto de Ley por la que se modifica la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (BOCG 27 de mayo 2011). Además de modificar la LGT, se realizan modificaciones en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD) y en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)[156].

El 30 de marzo de 2012, el Gobierno español aprobó el Real Decreto 13/2012, por el que se puso en práctica la Directiva sobre privacidad Modificado (Directiva 2002/58/CE modificada por la Directiva 2009/136/CE), relativa a las cookies.

El Real Decreto incluye los mismos criterios que figuran en el considerando 66 de la Directiva sobre intimidad y modificado, a excepción de la exigencia de una "acción afirmativa" a fin de lograr un consentimiento válido a través de la configuración del navegador. Este requisito adicional fue sugerido por el Grupo de Trabajo del Artículo 29 en su Dictamen 2/2010. España ha aplicado plenamente la nueva normativa de la UE sobre las cookies, pero además

[156] Transposición de la “Directiva de cookies”.
http://descargalegal.blogs.lexnova.es/2011/06/08/transposicion-de-la-directiva-de-cookies/
Página visitada 9 de junio de 2011.

impone criterios más restrictivos sobre el consentimiento de los usuarios expresada por la configuración del navegador o la configuración a equivalentes en otras aplicaciones. España sigue los criterios del Grupo de Trabajo a este respecto en el fortalecimiento del "opt-in" como requisito del consentimiento[157].

Así, las modificaciones a la LSSI son las siguientes[158]:

1.- Se añade un nuevo apartado 4 al artículo 20:
*«4. En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo.»*

2.- Se añade un nuevo párrafo al apartado 2 del artículo 21
*«Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.»*

3.- Se modifica el **artículo 22**
*«Artículo 22. Derechos de los destinatarios de servicios.*

*1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.*

*A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.*

*Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.*

*2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya*

157 http://www.twobirds.com/English/News/Documents/Spain_implements_EURegulation_Cookies.htm Página visitada 27 de abril de 2012.

158 http://brosaabogados.blogspot.com.es/2012/04/modificaciones-para-adaptar-la-lssi-la.html Página visitada el 14 de junio de 2012.

*facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

*Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.*

*Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.»*

## 2.6 Finlandia

En la actualidad, el uso de cookies se permite en Finlandia, siempre que el usuario esté debidamente informado de ello. Por otro lado, la modificación de la Directiva sobre privacidad ha planteado el debate sobre si su implementación en los Estados miembros tendrá algún impacto en el negocio de servicios de Internet, ya que la Directiva deja mucho espacio para la interpretación de los legisladores nacionales. En Finlandia, un punto de vista similar al Considerando 66 parece haber sido adoptado en la propuesta de proyecto del gobierno. La versión del texto propuesto de la Ley de Privacidad en la e-comunicación (*Sähköisen viestinnän tietosuojalaki*) establece el requisito del consentimiento del usuario para el uso de cookies por los proveedores de servicios de Internet. Sin embargo, el proyecto de propuesta gubernamental establece que el consentimiento puede ser recibido a través de la configuración del navegador, ya que los servicios de Internet deben ser fáciles de usar. Finlandia fue uno de los pocos Estados miembros que llevaron a cabo los cambios a la Directiva sobre la privacidad dentro de los plazos requeridos, es decir, al 25 de mayo de 2011. El Parlamento finlandés aprobó los cambios de acuerdo con el proyecto de propuesta gubernamental. La ley actual requiere el consentimiento del usuario para el uso de cookies, y que tal consentimiento puede ser obtenida a través de la configuración del navegador. Esto supone que la configuración del navegador es fácil de usar, y que el consentimiento puede ser válidamente dado con sólo cambiar la configuración[159].

[159] "Implementation of E-Privacy Directive in Finland: Will User-friendliness Override Privacy in the Use of Cookies in Internet Services?" http://www.castren.fi/Page/c1ccbac8-1bad-436e-bb79-e1ffaa00df14.aspx?groupId=a0231459-d54f-4ff6-8057-

Vemos entonces que se está cumpliendo con la Directiva en virtud a la modificación de la Ley sobre la Protección de la Privacidad en las Comunicaciones Electrónicas Nº 1516/2005, encontrándose las normas relativas a las cookies incorporados en el § 7.

## 2.7 Francia

De conformidad con el artículo 17 de la Ley N° 2011-302, de 22 de marzo de 2011, la aplicación de la Directiva 2009/136/CE ha sido delegada por el Parlamento al Gobierno. Al 22 de marzo de 2011, el Gobierno francés ha dado seis meses para aplicar la Directiva. El período de consulta pública finalizó el 20 de mayo 2011.

La modificación se llevó a cabo por la Ordenanza N° 2011-1012 del 24 de agosto 2011 y se publicó en el Boletín Oficial francés el 27 de agosto relacionada con las comunicaciones electrónicas.

En esta implementación no sólo se define el régimen jurídico del uso de cookies, sino que también introdujo varias medidas para fortalecer el régimen ya estricto de la ley de privacidad francesa. De acuerdo con la Directiva de cookies, el Código francés de Correos y Telecomunicaciones establece que en los usuarios deben estar clara y plenamente informado de la finalidad de las acciones de (i) el acceso, a través de transmisión electrónica, a la información ya almacenada en su terminal o (ii ) la inscripción de la información en dicha terminal.

Los usuarios también deben ser informados de los medios disponibles para denegar tal acceso o inscripción. Tras la recepción de dicha información, el usuario debe expresar su acuerdo antes de la instalación o el uso de una cookie puede continuar.

La Ordenanza francesa establece, sin embargo que este consentimiento puede ser consecuencia de la utilización de los parámetros apropiados en el dispositivo de conexión o cualquier otro proceso bajo el control del usuario. Según lo permitido por la Directiva de cookies, esta disposición no será aplicable para el acceso o la inscripción de la información en la terminal en caso de dicho acceso o la inscripción tiene como único propósito permitir o facilitar la comunicación electrónica o de lo estrictamente necesario para el suministro de un servicio de comunicación en línea expresamente solicitada por el usuario. Concretamente, esto significa que los usuarios tienen que estar informados de la instalación y el uso de cookies, pero, en caso de que sus navegadores estén

034a2b359a33&announcementId=08376f5f-4441-4901-999a-b7d3d31be488#Artikkeli_1 Página visitada 16 de Julio de 2011.

configurados para permitir dicha información, no se ha de dar su consentimiento expreso para ello. Esta información tendrá que llevarse a cabo al menos antes de que la cookie se instalara por primera vez. La redacción del texto también podría interpretarse en el sentido de que el usuario debe ser informado cada vez que se accede a la cookie, pero esto parece muy poco práctico, como la CNIL (Autoridad Francesa de Protección de Datos) reconoció en su comunicación de fecha 5 de febrero de 2009. (…) La Ordenanza también creó un nuevo delito penal (que no fue requerida por la Directiva Cookies). Por último, el opt in antes de la obligación de envío de prospección de e-mails ya no se aplica a los individuos sino también a los usuarios o abonados, que por lo tanto, también incluye personas jurídicas[160].

De acuerdo a la orientación de la CNIL, el término "cookie" también se aplica a otro tipo de tecnología relacionada con las cookies, al igual que las cookies "Relámpago", también conocido como "Local Shared Objects", y el almacenamiento web local, también llamado almacenamiento DOM. El término "cookie" por lo tanto, tiene un amplio alcance. Sin el consentimiento necesario para tipos específicos de las cookies. Las siguientes cookies no son capturadas por la información y las reglas del previo consentimiento informado[161]:

- Las cookies que se utilizan para un carrito de compra en el sitio web de un minorista en línea;

- Las cookies de sesión de usuario (identificador de sesión), para vincular las acciones de un usuario necesarias para la prestación del servicio que ha solicitado;

- Cookies que tienen el único propósito de contribuir a la seguridad que el usuario ha pedido;

- Las cookies para el registro del idioma hablado por el usuario (para los sitios traducidos a muchos idiomas) u otras preferencias necesarias para prestar el servicio requerido;

- Cookies Flash que contienen los elementos estrictamente necesarios para reproducir una obra multimedia (audio o vídeo), si el contenido ha sido solicitado por el usuario.

La CNIL indica que, aunque no se requiere el previo consentimiento para este tipo de cookies, se recomienda, sin embargo, que los operadores brinden información sobre el uso de las cookies en la política de privacidad de su sitio

[160] "France implements the cookies directive and strengthens its privacy laws". http://trap.it/RqjXg5 Página visitada 10 de setiembre de 2011.
[161] http://www.itst.dk/sikkerhed/privacy/lagring-af-og-adgang-til-oplysninger-pa-andres-udstyr Página visitada 28 de abril de 2012.

web.

Respecto a las cookies de terceros, la información y el consentimiento no tiene que ser administrado dos veces. Por lo tanto, si una agencia de publicidad da la información y recoge el consentimiento del usuario de Internet, el operador encargado de la página web no tiene que repetir esta operación para la cookie en particular. Si el operador de la página web está establecido fuera de la Unión Europea, puede delegar la aplicación de las nuevas disposiciones a un representante con domicilio social en Francia. Este representante también puede ser responsable de los datos de los usuarios de Internet[162].

Para la CNIL el consentimiento de los usuarios de las cookies debe ser específico, no considerándose como tal la configuración del navegador que acepte todas las cookies sin distinguir su objetivo final.

Para la CNIL, los mecanismos para recoger el consentimiento del usuario puede tomar muchas formas, como por ejemplo: un banner en la parte superior de una página web (como el instalado en la página web del ICO), un área de aplicación para el consentimiento que se superpone a la página, posibilidad de marcar cuando se registra para un servicio en línea. La CNIL deja claro en su orientación que los ejemplos anteriores no son exhaustivos. Sin embargo, la CNIL también considera que las ventanas emergentes no son recomendables porque pueden estar bloqueadas por navegadores.

## 2.8 Holanda[163]

Es el proyecto de ley más estricto.

Para el uso de las llamadas cookies de la primera parte, de reconocer a los usuarios o abonados al visitar sitios web relacionados con las transacciones financieras, el usuario debe dar su consentimiento. Para colocar las cookies de terceros y cookies de rastreo, el usuario o abonado debe dar su consentimiento inequívoco.

Para procesar los datos sensibles adecuados para supervisar la conducta al navegar por Internet (por ejemplo, con respecto a la publicidad comportamental) el previo consentimiento debe ser dado por el abonado o usuario.

---

[162] http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/ Página visitada 28 de abril de 2012.

[163] Birds & Birds “Cookies: Implementation of the new Directive (26 September 2011)”. http://www.twobirds.com/English/Documents/Implementation%20of%20the%20new%20ePrivacy%20Directive%20_26%20September2011BirdBird%20(2).pdf Página visitada 6 de octubre de 2011.

La versión actual de los navegadores no hacen las distinciones requeridas por el proyecto de ley sobre cookies. Por lo tanto, en la actualidad, la configuración del navegador no se puede considerar suficiente para expresar el consentimiento.

La ley necesita la aprobación del Senado para entrar en vigor. El papel del Senado en la práctica se limita a la votación sobre la totalidad de la legislación en lugar de considerar las disposiciones individuales. El Senado decidirá en breve sobre el procedimiento, es decir, si se va a votar con o sin un debate. El Senado discutirá el proyecto de ley en mayo.

### 2.9 Hungría

El proyecto de ley no menciona el Considerando 66 de la Directiva relativa a la configuración del navegador u otras aplicaciones. Además, el consentimiento debe obtenerse antes del almacenamiento de datos y acceso a los mismos. El proyecto fue presentado al Parlamento el 10 de junio de 2011 y fue aceptado el 11 de julio de 2011. La enmienda fue firmada por el Presidente y publicada en el Boletín Oficial el 19 de julio de 2011. La cláusula de cookies ya requería el consentimiento después de una información clara y completa.

### 2.10 Italia

La ley de la delegación de la ejecución número 211, de fecha 15 de diciembre de 2011, empezó a regir a los 15 días siguientes a su publicación en el Diario Oficial de la República Italiana que fue el 2 de enero de 2012). Conforme a dicha ley, el Gobierno expedirá un decreto-ley, que aplicará la Directiva de la UE 2009/136/CE, con un plazo de 3 meses a partir de la entrada en vigor de la delegación de ley.

### 2.11 Polonia

El único cambio se refiere a la información dada. El usuario debe ser informado (sin ambigüedades y de forma fácilmente comprensible), antes de colocar las cookies acerca de:

a. la finalidad del propósito del almacenamiento de las cookies,

b. la forma de utilizar el contenido de las cookies,

c. el período de almacenamiento y de tener acceso a ellas,

d. el nombre del procesador de la información almacenada.

Un proyecto de ley fue elaborado por el Ministerio de Infraestructura el 13 de julio 2011. Las propuestas se encuentran actualmente en consulta por el gobierno y no han llegado al Parlamento todavía. La última versión de propuesta es del 12 de febrero 2012.

### 2.12 República Checa

La propuesta del gobierno fue del 5 de mayo de 2011 (Ref. Nº 347). Su primera lectura tuvo lugar el 15 de junio 2011.

La Directiva se aplica a través de enmiendas a la Ley de Comunicaciones Electrónicas por la Ley Nº 468/2011 Coll. La norma sobre cookies se incorpora en 89 (3).

### 2.13 Suecia

Al ingresar al sitio web http://www.sweden.gov.se aparece la siguiente leyenda:

*"El 1 de julio, entraron en vigor los cambios a la Ley de Comunicaciones Electrónicas (2003:389). Esto significa que los visitantes de un sitio web tienen que consentir activamente el almacenamiento de cookies en su ordenador. Las cookies se utilizan en la sweden.gov.se para garantizar que el sitio web sea lo más accesible y usable posible. Algunas cookies son necesarias para que sweden.gov.se pueda trabajar y ya se han almacenado temporalmente en su ordenador. Se eliminan cuando se cierra el navegador web. Usted puede bloquear las cookies de terceros, pero algunas secciones de la web pueden perder alguna funcionalidad. Más información sobre las cookies en sweden.gov.se Acepto almacenar las cookies en el ordenador".*

También en el sitio web de la Autoridad de Protección de Datos se solicita el consentimiento http://www.datainspektionen.se/in-english/publications/

### 2.14 UK

La legislación del Reino Unido sólo se refiere a la palabra "Abonado". No hay referencia a los "usuarios". El consentimiento para el uso las cookies expresado a través de configuración del explorador web, requiere que el destinatario activamente configure el navegador. Esta acción va más allá de la redacción del considerando 66 de la Directiva. Además de las configuraciones del navegador u otras aplicaciones, el consentimiento también puede ser expresado a través del programa directamente con referencia a los estándares de la industria destinados a recoger y gestionar su consentimiento.

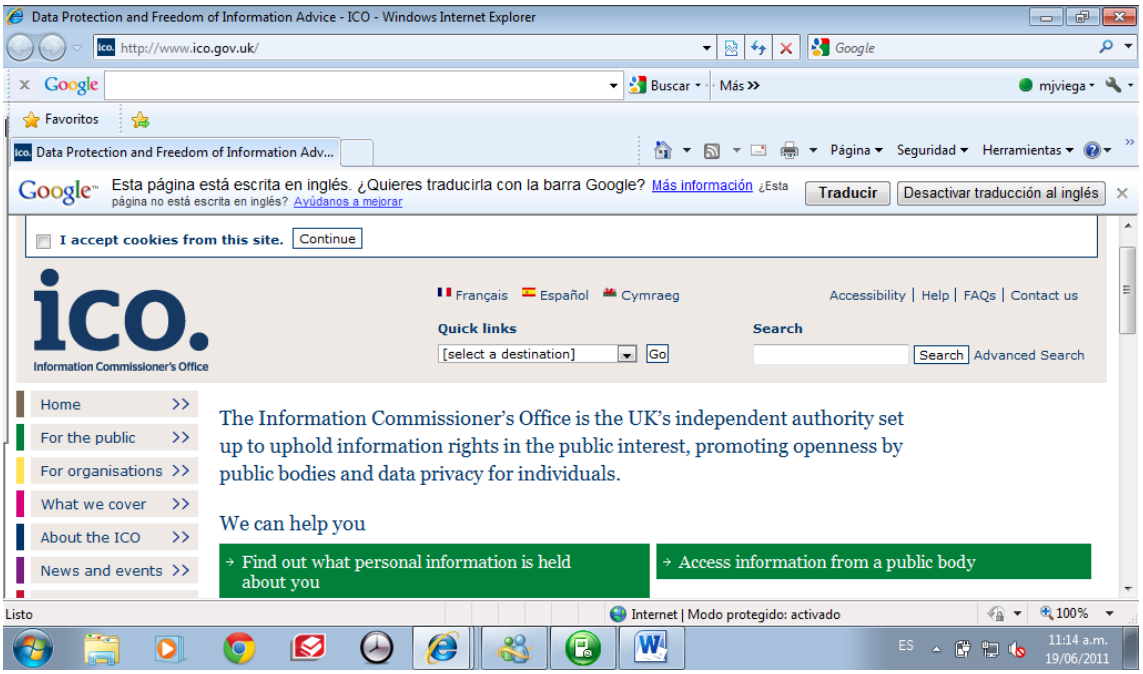
El consentimiento es dado por un abonado que modifica o establece controles sobre el navegador de Internet. Esto no cubre un usuario de Internet que no realiza ningún cambio en el valor predeterminado de la configuración del navegador.

La Directiva es implementada a través de la privacidad y las comunicaciones (Directiva CE) (Modificación) de 2011. El ICO publicó una Guía titulada "Cambios a las normas sobre el uso de las cookies y tecnologías similares para el almacenamiento de la información". A los operadores se les han dado 12 meses para cumplir con el nuevo requisito.

El Comisionado de la Información siendo el regulador del Reino Unido de las cuestiones de protección de datos, y, curiosamente, en ese código de práctica, que en realidad admite una opción de enfoque y dice que no hay nada intrínsecamente injusto o intrusivos sobre OBA. Y eso es una postura marcadamente diferente de la postura adoptada por el Grupo de Trabajo del Artículo 29. La buena práctica actual para la conducta para la publicidad en el Reino Unido se establece en los principios de buenas prácticas del Internet Advertising Bureau de OBA y que promueve el comportamiento en torno a tres fundamentos para proporcionar a los usuarios el aviso y dándoles opción a negarse y saber que es una opción, no opt in y que puede cambiar y también educar a los consumidores sobre los beneficios de la OBA. La directiva PEC establecer las reglas para las cookies, la directiva de protección de datos es aplicable a un proceso más general de los datos personales, pero las dos se superponen y es posible que la Directiva sobre protección de datos, cuando es examinada, puede inmiscuirse más en este ámbito. Esta es realmente la posición en el Reino Unido[164].

En el sitio web www.ico.gov.uk podemos observar la opción de aceptación de las cookies de este sitio, en la parte superior izquierda de la pantalla: "I accept cookies from this site".

[164] LEE, Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.




## 3. REFLEXIONES FINALES

Cuando comenzamos el presente trabajo hicimos hincapié en que el mismo poseía trascendencia económica, política, jurídica, además de los aspectos técnicos que se deben considerar y ahora podemos ver reflejado a todos ellos en las siguientes reflexiones.

### 3.1 Repercusiones económicas en la industria publicitaria en la web

Un aspecto a tener en cuenta es en cuanto a las repercusiones que la normativa y su aplicación tendrá en la industria de la publicidad, porque si se aplica una norma más severa en Europa que en otras partes del mundo, podría tener un impacto negativo sobre el número de empresas que se localicen en Europa, ya que muchas de ellas podrían optar por instalarse en otros países, ya que la globalización y el ciberespacio así lo permiten.

Está por verse como sigue, dice Mullock, pero es ahí donde estamos en este momento: mirando a los demás Estados miembros de la Unión Europea. Los holandeses han adoptado un enfoque similar. Otros Estados miembros todavía no muestran sus cartas. En particular, en Alemania ha habido una indicación de opt in como requisito principalmente de los reguladores alemanes, pero todavía

tenemos que ver en realidad el mejor proyecto. La ley aparece para el debate en Alemania como yo lo entiendo, dice James Mullock[165].

### 3.2 Regulación estricta & pago de la publicidad

Si la regulación en materia publicitaria es muy estricta puede suceder que tengamos menos publicidad. En ese caso, alguien tendrá que pagar por los servicios que se prestan gratuitamente en Internet. Ya hicimos mención en el presente trabajo que nada es gratis en la Red, que esto es solo la apariencia.

Así que, o el contenido o ciertos servicios desaparecerán en Internet o las personas estarán cobrando por ello, lo que implicará un cambio importante en el concepto actual de relacionamiento en la web.

### 3. 3 La configuración del navegador y el consentimiento

Algunos autores mantienen una postura favorable hacia el uso de la configuración del navegador como una solución para obtener el consentimiento a la instalación de las cookies.

Creo que confiar en los navegadores para recoger el consentimiento se podría entender como una delegación de la responsabilidad del cumplimiento. En última instancia, las personas que están instalando las cookies, y las personas que están recogiendo y utilizando esta información, van a ser las redes o los anunciantes, o los editores del sitio web, no los navegadores.

Por lo que me parece extraño, que una red de publicidad delegue esta responsabilidad para obtener el consentimiento en el navegador.

El Grupo de Trabajo del Artículo 29 manifestó muy claramente que el consentimiento debe ser específico e informado a la red de anuncios en particular o al uso específico del tratamiento que se está realizando y me parece que la configuración del navegador, por lo menos actualmente, no cumple con nuestros estándares, opina Lee. Esta es una tecnología que no depende de las cookies, pero puede identificar a los usuarios a un sitio web basado en la huella digital única de ese navegador. En esencia, la forma en que funciona es lo que parece en la configuración de todo el navegador: el navegador que está usando, con qué sistema operativo está trabajando, las fuentes que ha instalado en su ordenador, la resolución de pantalla, todo ese tipo de cosas. En general, si usted toma el suficiente número de configuraciones le permitirán identificar a los usuarios individualmente. El

[165] MULLOCK, James. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

peligro es lo que una opción de "cookies", porque las empresas empiezan a confiar más en la toma de huellas dactilares digitales y menos en las cookies. Las huellas digitales en general son menos transparentes a los consumidores porque no saben lo que está sucediendo, ellos no ven cookies en sus máquinas, que no puede bloquear huellas digitales de la forma en que pueden con las cookies[166].

### 3.4 ¿Quién es responsable por el tratamiento de los datos personales?

Cuando mencionamos los sujetos que interactúan en el marketing comportamental en línea dijimos que tenemos anunciantes, tenemos las redes de publicidad y los editores.

La pregunta que debemos hacernos es: ¿quién es el responsable del tratamiento? ¿Quién es legalmente responsable por el procesamiento de los datos?

A partir del análisis que hemos realizado, podemos concluir que los anunciantes en general no son responsables del tratamiento. Podrían serlo en algunos casos, por ejemplo, si las redes de anuncios transmiten información extra al anunciante o incluso si el propio editor encuentra una forma de transmitir información acerca de la persona para el anunciante.

Tampoco Mullock cree que en este momento los anunciantes podrían tener el papel de los responsables del tratamiento. Y también coincidimos con él en que las redes de publicidad son claramente los responsables del tratamiento. Ellos son los que van a colocar las cookies, procesar las direcciones IP, crear perfiles, los usuarios de rastreo, entre otros. Y luego está la cuestión de los editores. Creemos que los editores tienen un papel muy limitado, pero existente como el tratamiento de datos, ya que permiten la transferencia de la dirección IP del usuario a terceros, aquí está la red de publicidad. Ellos también tienen responsabilidad en este caso, por la transferencia de información a la red de anuncios. Así que ahora tenemos dos personas que son responsables por algo. La pregunta es: ¿quién debe proporcionar la información a los usuarios? Creemos que es necesaria la cooperación entre la red de anuncios y la editorial[167].

### 3.5 ¿Cuáles son las directrices que proporciona el Grupo de Trabajo del Artículo 29 en materia de cookies?

[166] LEE, Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

[167] MULLOCK, James. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

En primer lugar, el consentimiento fundamentado previo no es necesario para cada página web que utilice cookies determinadas. Se quiere evitar el temor de que se repitan las ventanas emergentes.

Creo que la Directiva le da elementos para creer que una vez que usted otorga su consentimiento para una cookie, también lo da para la lectura y modificaciones posteriores de la cookie, se entiende que el acuerdo sigue siendo válido. Pero también hay que tener presente que este tipo de consentimiento no debe ser para siempre, el usuario tiene que poder revocarlo.

En segundo lugar: el deber de informar. Esta información deberá, como mínimo, explicar con claridad la identidad de la red de publicidad, la finalidad del tratamiento, los datos que está recogiendo, y se debe recordar al usuario que periódicamente se está supervisando.

Por último: el Grupo de Trabajo del Artículo 29 cree firmemente que el OBA no debe aplicarse a los niños porque son más vulnerables y no están en condiciones de comprender plenamente y dar su consentimiento a las cookies.

## 3.6 Alcance del concepto cookies

Si bien hemos hablado del concepto cookies, de las distintas clases y categorías, hay autores, como es el caso de Zorba[168], que se cuestiona en términos de lo que sería aceptable como "cookies" o no, y manifiesta que como abogado está muy inseguro de lo que sería aceptable en términos de lo que podríamos llamar "cookies técnicas".

Sobre todo, se basa en el Dictamen 2008/C/181/01 del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica, entre otras, 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 (Directiva sobre intimidad y comunicaciones electrónicas) que dice: "Veo las cookies técnicas como un conjunto muy limitado de "cookies ", ni siquiera "cookies" que facilitarían la transmisión de información excluyendo las cookies de configuración de idioma, por ejemplo, y dejar a un lado otras cookies, por supuesto".

En los numerales 50 y 51 del Dictamen se establece lo siguiente[169]:

[168] ZORBA, Kimon. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

[169] http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2008:181:SOM:es:HTML Página visitada 16 de febrero de 2011.

*50. El SEPD considera conveniente eximir de la necesidad de informar y de dar la posibilidad de negarse a la recogida de información propia en situaciones como las ilustradas, cuando el almacenamiento o el acceso de índole técnica al terminal del usuario son necesarios para el solo fin de transmitir la comunicación por una red de comunicaciones electrónicas. Lo mismo ocurre cuando el acceso o el almacenamiento técnicos son estrictamente necesarios para proporcionar un servicio de la sociedad de la información. Sin embargo, el SEPD no ve la necesidad de excluir de la obligación de informar u ofrecer la posibilidad de negarse en las situaciones en que el almacenamiento o acceso técnicos sirven simplemente para facilitar la transmisión de una comunicación. Por ejemplo, de conformidad con la última oración de este artículo, un titular de datos no puede beneficiarse de la información ni del derecho de negarse al tratamiento de sus datos si un chivato recoge sus preferencias lingüísticas o su ubicación (por ej. Bélgica, China), ya que este tipo de chivato puede presentarse como destinado a facilitar la transmisión de una comunicación. El SEPD sabe que, en lo que atañe a los programas de ordenador, en la práctica se da a los titulares de datos la posibilidad de negarse al almacenamiento de chivatos o a modularlo. Sin embargo, esto no está respaldado con suficiente claridad por ninguna disposición jurídica que capacite formalmente al titular de los datos para defender sus derechos en la situación recién descrita.*

*51. Para evitar esa consecuencia, el SEPD sugiere una modificación mínima en la última parte del artículo 5.3, consistente en la supresión de la palabra «facilitar» de la oración: «no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar un servicio de la sociedad de la información […]».*

El siguiente cuestionamiento es si la tecnología arreglará este tema. Zorba no está de acuerdo, porque no cree que el mágico navegador que el Grupo de Trabajo del Artículo 29 tiene en mente vaya a ser desarrollado.

Y analiza otros problemas fundamentales con el enfoque del navegador. En primer lugar, se hace del fabricante del navegador el guardián de Internet. Esto es de poca visión, porque no quiere convertirse en la Internet de solo unas pocas empresas. Al final, sería también un mandato de la tecnología. Creo que todo el mundo coincide en que la Directiva 95/46/CE es tecnológicamente neutra. “Veo que existe un problema real aquí, porque si vamos por la línea de ordenar o hacer del navegador el tema clave principal para la gestión de las cookies, básicamente excluimos otras tecnologías que puedan surgir. Creo que lo que el Grupo de Trabajo del Artículo 29 ha sugerido es una carga excesiva y en la práctica no funcionará”[170].

[170] ZORBA, Kimon. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

Personalmente creo que la transparencia es una buena solución para los usuarios, puede ser dinámica, puede ser en un contexto específico y estar presente en todo momento. Creo que es necesario pensar en la posibilidad de hacerlo a través de un ícono, como lo establece el sitio de la ICO, o pensar en otras posibilidades que den seguridad, confianza y respaldo, como se establece en el Dictamen 16/2011 del GT29.

### 3.7 ¿Existen soluciones para las diferentes amenazas?

Las soluciones podemos analizarlas desde dos instancias diferentes: en primer lugar como formas de prevenir estos problemas, de evitar los intrusos en nuestros sistemas, de bloquear el acceso a los espías a nuestro ordenador. En esta instancia contaremos con la seguridad informática, ya que la misma tecnología nos da herramientas para contrarrestar los ataques, a través de software especializado, la encriptación de datos cuando no es considerada "tecnología de doble uso", entre otras.

Pero también, en el ámbito preventivo, se hace necesario estar informados de las regulaciones jurídicas en la materia. Aquí no nos referimos únicamente a la Declaración de Derechos Humanos o a la Constitución de la República como normas que protegen nuestros Derechos Fundamentales. Nos referimos a las medidas preventivas a la hora de realizar contratos informáticos o telemáticos, a la implementación de estrategias para disminuir el impacto de estos ilícitos a nivel empresarial. A estar preparados para que de producirse un fraude, puedan trabajar el área jurídica e informática en forma coordinada y eficaz para no perder evidencias digitales, para determinar los culpables en la esfera penal y para recuperar activos cuando hay pérdidas materiales.

Es necesario generar conciencia de que nosotros somos los primeros custodios de nuestros datos personales y de la información de nuestra propiedad, que debemos estar alertas, de la misma forma que lo estamos con nuestros bienes materiales, ya que es posible que en forma disimulada, "alguien" nos esté observando.

Europa ha regulado el tema con carácter general y los países de la Unión Europea enfrentaron o enfrentan el desafío de incorporar la Directiva. Pero aunque a veces las soluciones pueden resultar confusas, tenemos que tener presente que más allá de las modalidades del tratamiento de datos, de lo "novedosa" que pueda parecer la herramienta, es fundamental el cumplimiento de los principios de la protección de datos personales como garantía para todos nosotros. Son NUESTROS datos, SOMOS nosotros mismos y por tanto solo NOSOTROS podemos autorizar la creación de perfiles y la manipulación de la información personal.

# INDICE

3.5 ¿Cuáles son las directrices que proporciona el Grupo de Trabajo del Artículo 29 en materia de cookies?

3.6 Alcance del concepto cookies

3.8 ¿Existen soluciones para las diferentes amenazas?

## BIBLIOGRAFIA

ACED FÉLEZ. Subdirector General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM). "EUROPRISE: Certificados de Protección de Datos para Europa". http://www.borrmart.es/articulo_redseguridad.php?id=1784 Página visitada 10 de octubre de 2011.

ALVAREZ-CIENFUEGOS SUAREZ, José María. "La defensa de la intimidad de los ciudadanos y la tecnología informática". Aranzandi 1999. Colección Divulgación Jurídica.

AMOR Daniel. "La (R)evolución. E-business. Claves para vivir y trabajar en un mundo globalizado". Prentice Hall. Buenos Aires, 2000.

ANXO TATO PLAZA. "Internet, a Publicidade e a Concorrencia" en Temas de Direito da Informática e da Internet. Coimbra Editora. 2004. Página 182.

ARAGON REYES, Manuel y FERNANDEZ ESTEBAN, María Luisa. Incidencia de Internet en los Derechos Fundamentales. Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid).

Birds & Birds "Cookies: Implementation of the new Directive (26 September 2011)".
http://www.twobirds.com/English/Documents/Implementation%20of%20the%20new%20ePrivacy%20Directive%20_26%20September2011BirdBird%20(2).pdf
Página visitada 6 de octubre de 2011.

BRINN, Laura. "Brain Scans Could Be Marketing Tool Of The Future. The may nor replace the focus group, but could reveal new information". Thurday, March 4, 2010. www.dukenews.duke.edu/2010/03/brainscan.html Página visitada el 14 de junio de 2010.

BUGALLO, Beatriz. "Nuevos usos en la sociedad de la información". Conferencia dictada en el Simposio organizado por Antel sobre Ética e Internet, sección "Internet y los cambios de la vida cotidiana". Radisson, 2000. http://beatriz.bugallo.info

CAMPBELL, Duncan. "Interception Capabilities 2000".
http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm

CAS, Johann. "Computación ubicua, privacidad y protección de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes". Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009.

DE LA VEGA GARCIA, Fernando L. “Datos personales y deberes del empresario en la publicidad”. Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009.

DELPIAZZO, Carlos y VIEGA, María José. “Lecciones de Derecho Telemático. Tomo II”. Fundación de Cultura Universitaria. Montevideo, marzo 2009.

DELPIAZZO, Carlos y VIEGA, María José. “Lecciones de Derecho Telemático”. Tomo I. Fundación de Cultura Universitaria. Lección 8. Montevideo, abril de 2004.

DELPIAZZO Carlos. “Dignidad Humana y Derecho”. Universidad de Montevideo. Facultad de Derecho. Montevideo, 2001.

DE MIGUEL ASENCIO, Pedro Alberto. “Derecho privado de Internet”. Editorial Civitas. Tercera edición actualizada. Madrid, 2002.

GARCIA MORALES María Jesús. “Poderes públicos, autorregulación y protección del consumidor en Internet: a propósito de la regulación del distintivo público de confianza”. Capítulo del libro Consumidores y usuarios ante las nuevas tecnologías. Lorenzo Cotino Hueso (coordinador). Derecho y tic’s. Valencia, 2008. Página 280.

GARCIA MOSTAZO, Nacho. “Libertad vigilada. El espionaje de las comunicaciones”. Ediciones B Grupo Z. Barcelona, enero 2003.

GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 1/2010 de 16 de febrero de 2010 sobre los conceptos de “responsable del tratamiento” y “encargado del tratamiento”.

GUNCKEL, Tony. Vicerrector Universidad Tecnológica de Chile INACAP. Sede Rancagua. http://eltipografo.cl/2011/04/facebook-y-el-marketing-digital-en-el-2011/ Página visitada el 20 de abril de 2011.

IRUZUBIETA, Gonzalo. Director de Marketing y Comunicación de IAB SPAIN. “Debemos fomentar siempre el marketing interactivo en todas nuestras actuaciones”. Diario digital de marketing y publicidad en español. Puromarketing. 14 de octubre del 2008.

LEE Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

LOPEZ GARCIA, Mabel. “La publicidad y el derecho a la información en el comercio electrónico”. Editado por eumed.net; accesible a texto completo en html://www.eumed.net/cursecom/librería (2004).

LOPEZ, José Luis. “El FBI y sus troyanos”. http://www.vsantivirus.com/22-11-01b.htm Página visitada 13 de junio de 2005.

LLANEZA GONZALEZ Paloma. “Internet y Comunicaciones Digitales. Régimen legal de las tecnologías de la información y la comunicación”. Bosch. Barcelona, abril 2000.

MANZANARES GALEAN, Llanos y otro. “Implicaciones de la protección de datos en el marketing”, en MK Marketing+Ventas N° 199, Febrero de 2005. Página 22. http://pdfs.wke.es/8/7/8/6/pd0000018786.pdf

MASTER UNIVERSITARIO “Asesoría Legal en Tecnologías de la Información”. Curso on line de la Universidad Politécnica de Valencia. Tema: “Marketing y Publicidad en Internet”. Marzo 2005.

McLURE, Charles E., Jr. y CORABI, Giampaolo. “La tributación sobre el comercio electrónico: objetivos económicos, restricciones tecnológicas y legislación tributaria”. Depalma. Buenos Aires, 2000.

MEEKER, Mary. “La publicidad en Internet”. Ediciones Granica, 2001.

MILLAR Michael. “Cookie: monster? How will business cope with new laws”. http://www.bbc.co.uk/news/business-13951107 . Página visitada el 7 de julio de 2011.

MULLOCK, James. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

ORWN George. 1984. Ediciones Destino. Barcelona. Séptima edición, junio 1984.

O'BRIEN Kevin J. “Estableciendo límites de privacidad en Internet”. Publicado 18 de septiembre 2011 http://www.nytimes.com/2011/09/19/technology/internet/setting-boundaries-for-internet-privacy.html?_r=3 Página visitada el 19 de setiembre de 2011.

PALADELLA SALORD, Carlos. “Datos personales contenidos en bases de datos y registros electrónicos. REDI número 7 de febrero de 1999.

PALAZZI Pablo A. “La protección de los datos personales en la Argentina. Ley 25.326 de protección de datos personales y hábeas data comentada y anotada con jurisprudencia”. Editorial Errepar. Argentina 2004.

PANIZA FULLANA, Antonia. "Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores". Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009.

PANNETRAT, Allan. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

PEINADO GRACIA Juan Ignacio. Prólogo del libro "La protección de los destinatarios de las comunicaciones comerciales electrónicas" de Trinidad Vázquez Ruano. Marcial Pons. Madrid, 2008.

PROTANLINSKI, Emil. "Facebook fixes cookie behavior after logging out". http://www.zdnet.com/blog/facebook/facebook-fixes-cookie-behavior-after-logging-out/4120 Página visitada 4 de octubre de 2011.

REBOLLO DELGADO, L y SERRANO PEREZ, M: "Introducción a la protección de datos". 2ª Edición. Madrid, 2008.

RIOS Mauro. "El pequeño empresario en América Latina y el Caribe, las TIC y el comercio electrónico".

RIOS Mauro D. "Des espaldas al Chip. Breves guías de cómo ver la tecnología". Montevideo, Mayo 2000.

RIVAS ALEJANDRO, Javier. "Aspectos Jurídicos del Comercio Electrónico en Internet". Editorial Aranzadi. Segunda reimpresión, octubre 2000. Página 51.

ROBERTS Mac, FLINT David y SURGENOR Valerie. Tiempo de crisis cookies: código de publicidad nuevo no cumple con la legislación de las cookies de la UE? Reino Unido, 14 de septiembre 2011. http://www.lexology.com/library/detail.aspx?g=e02b32af-d99e-4f00-89f2-af0c210d98a2&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Itechlaw+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2011-09-19&utm_term= Página visitada el 19 de setiembre de 2011.

RUBI NAVARRETE, Jesús. Curso CEDDET: "El Derecho a la protección de datos personales, 1ª edición". Módulo 4. Tratamientos específicos (I). Marketing. Telecomunicaciones. Solvencia patrimonial. Tratamiento de Datos en el ámbito de la salud.

SZAFIR, Dora. “Consumidores. Análisis exegético de la ley 17.189”. Fundación de Cultura Universitaria. Montevideo, julio 2000.

TEAHAN, Mary. Presentación en el VII Seminario Nacional e Internacional “La protección de datos personales: una herramienta para el desarrollo económico” Buenos Aires, 22 de abril de 2010.

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES. Libro de Resoluciones, dictámenes e informes. Año 2009.

VAZQUEZ RUANO Trinidad. “La protección de los destinatarios de las comunicaciones comerciales electrónicas”. Marcial Pons. Madrid, 2008.

VICTORIA MAS JUAN Salvador. “Introducción a la comunicación interactiva. La Publicidad como ejemplo del Nuevo Paradigma de la Comunicación. Capítulo del libro Consumidores y usuarios ante las nuevas tecnologías. Lorenzo Cotino Hueso (coordinador). Derecho y tic’s. Valencia, 2008. Página 467.

VIEGA, María José. “Privacidad en Internet”. Derecho Informático. Tomo II. Año 2001. Fundación de Cultura Universitaria. Montevideo, 2002.

VIEGA, María José. “e-Marketing”. Ponencia presentada y publicada en las Memorias del XI Congreso Iberoamericano de Derecho e Informática. Panamá, 19 al 23 de junio de 2006.

VIEGA, María José. “Protección de datos y delitos informáticos”. Ponencia presentada al III Congreso Internacional de Derecho. Bolivia, 10 al 13 de setiembre de 2003 y publicada en el Libro de Memorias de dicho Congreso.

VIEGA, María José. *“*El problema de los datos personales y el espionaje en Internet*”*. Cuarto Congreso Internacional de Derecho (CIDER 2005) en las Sedes de Cochabamba, Santa Cruz y La Paz. Bolivia, 23 al 25 de noviembre de 2005. Publicada en el Libro de Ponencias.

VIEGA, María José. “Derechos Humanos en el Ciberespacio”. Trabajo publicado en la Revista electrónica de Derecho Informático (REDI), Junio de 2002.

VIEGA, María José. “Privacidad en Internet”. Derecho Informático. Tomo II. Fundación de Cultura Universitaria. Montevideo, 2001.

VIEGA, María José. “Delitos informáticos: manipulación de la información pública y privada”. II Jornadas Rioplatense de Derecho Informático. Buenos Aires, 18 de agosto de 2011.

VIEGA María José y CARNIKIAN Federico. “Respuesta a los delitos informáticos: su visión desde la privacidad y la seguridad de la información”. Ponencia presentada al Seminario Nuevas Tecnologías: Privacidad y Seguridad. Cartagena de Indias, 21 al 23 de julio de 2010.

VIEGA María José. “El marketing comportamental en línea desde la óptica de la protección de datos”. Ponencia presentada al Primer Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática. CIIDDI 2011. Mar del Plata, Argentina. 1, 2 y 3 de diciembre de 2011.

VIEGA, María José. Comentario de la conferencia realizada en el blog. http://mjviega.viegasociados.com

VIEGA María José. “Marketing comportamental en línea”. Conferencia dictada en las Jornadas Académicas del Instituto de Derecho informático. Montevideo, 15 y 16 de junio de 2011.

ZIMMERMANN, autor del paquete criptográfico PGP, citado por García Mostazo Nacho en “Libertad Vigilada. El espionaje de las comunicaciones”. Ediciones B. Barcelona, 2003.

ZORBA, Kimon. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

http://www2.noticiasdot.com/publicaciones/2006/0406/2104/noticias/noticias_210406-17.htm Página visitada el viernes 21 de abril de 2006.

http://www.elpais.com/articulo/internet/publicidad/online/crece/554/durante/2007/elpeputec/20080305elpepunet_4/Tes Página visitada 6 de marzo de 2008.

www.iprhelpdesk.org/controlador.jsp?cuerpo=noticiasCuerpo&seccion=noticiaseventos&tipoListado=all&id=0000005588&len=es Página visitada 1 de mayo de 2005.

http://www.ipro.com/ I/PRO - *Internet Profiles Corp*. Página visitada 2 de diciembre de 2006.

www.milliondollarhomepage.com Página visitada el 13 de enero 2006.

http://marketingcausaefecto.typepad.com/thetrickypart/2005/12/milliondollarho.html Página visitada el 13 de enero 2006.

http://www.milliondollarwomenshomepage.com Página visitada el 13 de enero 2006.

http://www.millionpennyhomepage.com Página visitada el 13 de enero 2006.

http://dhost.info/veducm/alquilatupixel/index.htm Página visitada el 2 de diciembre de 2006.

http://www.autocontrol.es/pdfs/NP%20Asociacion%20Confianza%20Online.pdf Página visitada 12 de junio de 2010.

http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/04-01.htm Directiva número 6 del Consejo de Seguridad Nacional sobre Inteligencia (NSCID nº 6). "La Agencia de Seguridad Nacional y el Servicio Central de Seguridad". Departamento de Defensa de Estados Unidos, 23 de diciembre de 1971.

www.askcalea.net Página visitada el 13 de junio 2005.

http://facultyweb.maconstate.edu/jashford/Class%20projects/6pmclass/CarnivorePaperandQuestions.doc "Carnivore: The FBI's Email Sniffer".

http://www.larazon.es/lared/laredesoias.htm y El Parlamento europeo reconoce la existencia de la red de espionaje Echelon.

http://idg.es/pcworld/noticia.asp?id=18239.

http://www.noticiasdot.com/publicaciones/2005/0105/2001/noticias200105-24.htm Página visitada jueves 20 enero 2005.

www.noticiasdot.com Página visitada el 19 de abril de 2004.

http://www.noticiasdot.com/publicaciones/2005/0205/0202/noticias020205/noticias020205-09.htm Página visitada el 2 de febrero de 2005.

www.noticiasdot.com "La cara oculta de Google: Afirman que viola la privacidad de los usuarios y vigila sus actividades online". Página visitada el 30 de abril de 2004.

http://www.noticiasdot.com/publicaciones/2004/0404/2104/noticias210404/noticias210404-7.htm

http://www.hispasec.com/unaaldia/2410 Página visitada el 13 de junio de 2005.

http://www.noticiasdot.com/publicaciones/2005/0205/0902/noticias090105/noticias090205-15.htm Página visitada el 9 de febrero de 2005.

http://www.noticiasdot.com/publicaciones/2005/0205/0902/noticias090105/noticias090205-15.htm Página visitada el 9 de febrero de 2005.

http://www.hispasec.com/unaaldia/2406 Página visitada el 13 de junio de 2005.

http://www.mx.terra.com/tecnologia/interna/0,,OI889426-EI4906,00.html Página visitada 21 de junio de 2010. El Pharming: amenaza de fraude a negocios. Trend Micro. 21 de febrero de 2006.

http://www.laflecha.net/canales/seguridad/articulos/pharming/ El Pharming, un peligro para la e-banca. Página visitada 21 de junio de 2010.

http://ricoveri.ve.tripod.com/ricoverimarketing2/id47.html Página visitada el 4 de agosto de 2011.

http://www.serviciosadomicilio.cl/diccionario-internet/click-through.htm Página visitada 14 de julio de 2011.

http://www.fedma.org

http://todonoticiaslopd.com/2009/11/17/171109-a-punto-de-ver-la-luz-la-directiva-europea-de-proteccion-de-datos/ Página visitada el 12 de junio de 2010.

http://www.sip.gob.mx/noticias-sobre-tendencias/462-union-europea-quiere-poner-cerco-a-las-cookies Página visitada 12 de junio de 2010.

http://www.nytimes.com/2011/09/19/technology/internet/setting-boundaries-for-internet-privacy.html?_r=3 Página visitada el 19 de setiembre de 2011.

http://www.youronlinechoices.com/es/cinco-consejos-clave/ Página visitada el 19 de setiembre de 2011.

http://www.informationcommissioner.gov.uk/cms/DocumentUploads/what%20are%20personal%20data%20research.pdf

https://www.european-privacy-seal.eu/about-europrise/project-fact-sheet/fact-sheet-es.html
https://www.european-privacy-seal.eu/about-europrise/project-fact-sheet/fact-sheet-es.html Página visitada 1 de octubre de 2011.
"Position paper on the impact of the new "Cookie Law" on certifiability of behavioural advertising systems according to EuroPriSe". Julio 2010.
http://descargalegal.blogs.lexnova.es/2011/06/08/transposicion-de-la-directiva-de-cookies/ Transposición de la "Directiva de cookies".Página visitada 9 de junio de 2011.
http://www.castren.fi/Page/c1ccbac8-1bad-436e-bb79-e1ffaa00df14.aspx?groupId=a0231459-d54f-4ff6-8057-034a2b359a33&announcementId=08376f5f-4441-4901-999a-b7d3d31be488#Artikkeli_1 "Implementation of E-Privacy Directive in Finland:

Will User-friendliness Override Privacy in the Use of Cookies in Internet Services?" Página visitada 16 de Julio de 2011
http://trap.it/RqjXg5 "France implements the cookies directive and strengthens its privacy laws". Página visitada 10 de setiembre de 2011.

http://www.itst.dk/sikkerhed/privacy/lagring-af-og-adgang-til-oplysninger-pa-andres-udstyr Página visitada 28 de abril de 2012.

http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/ Página visitada 28 de abril de 2012.