UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PROCESAL

ANÁLISIS COMPARATIVO DE COOKIES Y LA PROTECCIÓN DE DATOS PERSONALES

AUTOR:
ALEX MEYER-PANTIN THOMAS
PROFESOR GUÍA: LORENA DONOSO A.
SANTIAGO, OCTUBRE 2004

INTRODUCCIÓN

Todo usuario de Internet se ha visto enfrentado alguna vez a mensajes de correo no solicitados, y se ha preguntado de qué modo el remitente obtuvo su cuenta de correo, como también le ha llamado la atención la atractiva oferta contenida en el mensaje. Más comunes aún, son los afiches de propaganda que aparecen en las páginas web, los cuales casi siempre se relacionan a la edad, sexo, e intereses del usuario. Por ejemplo, ofertas de suscripción a sitios eróticos aparecerán en los afiches publicitarios virtuales cuando el navegante sea hombre. La razón es muy sencilla, los publicistas saben quien es el navegante y donde se encuentra. ¿Cómo logran esto los comerciantes electrónicos y los publicistas de internet? A través de una tecnología denominada "cookies", un fichero de texto que algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, con información acerca de lo que hemos estado haciendo por sus páginas. En otras palabras, las cookies constituyen una potente herramienta empleada por los servidores Web para almacenar y recuperar información acerca de sus visitantes. Dado que el Protocolo de Transferencia de Hipertexto (http) es un protocolo sin estados (no almacena el estado de la sesión entre peticiones sucesivas), las cookies proporcionan una manera de conservar información entre peticiones del cliente, extendiendo significativamente las capacidades de las aplicaciones cliente/ servidor basadas en la Web. Mediante el uso de cookies se permite al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etc. De este modo, los publicistas virtuales utilizan la información recabada por la cookie para establecer un perfil del usuario basado en las páginas que visita más frecuentemente, y consiguientemente, utiliza ese perfil para presentarle avisos virtuales al usuario cada vez que se conecte, como también para enviarle correo con ofertas de productos.

El concepto tradicional de invasión a la privacidad usualmente se traduce en personas espiando a través de una ventana o revisando en forma ilícita el correo tradicional. Los atentados a la privacidad en Internet son sumamente sutiles, y que la mayoría de las veces ni siquiera son percibidas por las personas, ya que los mecanismos tecnológicos para supervigilar las conductas de los navegantes en la red están diseñadas de modo que no se les notifica al usuario de su existencia. En el derecho de hoy, la privacidad se clasifica en cuatro categorías básicas: 1) privacidad en la información; 2) privacidad corporal; 3) privacidad en las comunicaciones, y 4) privacidad territorial [1]. El tema primordial en Internet es la privacidad de la información, conocido también como **protección de datos**, la cual se define como el derecho de un individuo para controlar la adquisición, divulgación, y el uso de información personal.

Las cookies pueden violar la privacidad del usuario de internet primordialmente de dos maneras a través de una página web. Primeramente, las cookies son guardadas en el disco duro del usuario, dejando la posibilidad de tener acceso a ellas. Una vez que se tiene acceso a ellas, las cookies exhibirán detalladamente todos los sitios web que fueron visitados por ese computador dentro de un período de tiempo determinado. Además, el texto del archivo cookie pueda revelar información personal del usuario, como su clave, la dirección de e-mail, o cualquier otra información que fue inscrita mientras se visitaba el sitio. Un ejemplo de lo descrito ocurrió recientemente cuando funcionarios del Estado norteamericano descubrieron que John Deutch, antiguo jefe de la CIA, usaba el computador de su hogar para escribir memos ultra secretos. Tras

[1] NOTAS Sheri Hunter, Defamation and Privacy Laws Face the Internet, Comms. Law., Fall 1999.

una investigación que realizó el FBI de su computador personal para determinar el daño hecho a la seguridad nacional, se encontraron cookies que indicaban que desde su computador había visitado sitios para adultos, divulgando información de enorme relevancia para la CIA[2].

La segunda manera en que las cookies afectan la intimidad es a través de los servidores de los sitios web, los cuales también pueden percibir datos personales guardados en un determinado cookies cuando el usuario vuelve a visitar el mismo sitio. Mediante la cookie, las páginas web tienen la habilidad de determinar de qué sitio provino el usuario, los links que cliqueó mientras visitaba el sitio, las compras que realizó, y cualquier información personal que introdujo. Muchas cookies además tienen la facultad de identificar el IP (internet protocol address) del usuario, y por ende, permitiendo determinar la ubicación exacta del computador utilizado para acceder al sitio.

Una vez que el sitio reúne los datos personales, puede utilizarlos de tal manera que viole la vida privada de la persona. Por ejemplo, una mujer decide comprar un test de embarazo a través de la red, pensando que es una forma de asegurar su anonimato respecto de un asunto tan privado. Sin embargo, el sitio podría optar por divulgar el hecho de la compra junto a su correo electrónico a organizaciones pro vida, las cuales podrían saturar su correo con mensajes.

Otro método a través del cual se manifiestan las cookies en Internet es a través de “banner ads” o anuncios de publicidad que las compañías de marketing exhiben en la red. El caso públicamente más conocido y que llegó hasta los tribunales de los Estados Unidos fue el litigio de DoubleClick (se analizará más adelante), compañía de publicidad que fijaba sus banner ads en las páginas web de otras compañías. Estos anuncios persiguen un doble objetivo: publicitan los productos de los clientes de DoubleClick, y al mismo tiempo recolectan información a través del uso de cookies, respecto de cualquier persona que viste la página en que se exhiba el anuncio publicitario.

Mientras la mayoría de los sitios de internet tienen solamente la limitada capacidad para leer los cookies guardados en el disco duro de un usuario que visitó en el pasado su página, los “banner ads” tiene una mayor capacidad para vigilar la conducta de los usuarios en la red. Estos anuncios pueden ser publicados en cientos de páginas diferentes, y enviar sus propias cookies, además de las cookies enviadas por la propia página. Por lo tanto, las compañías dueñas de estos banner ads pueden recolectar considerables cantidades de datos personales de toda clase de usuarios. Esta potencial amenaza a la privacidad que significan las cookies de los avisos publicitarios se refleja en un estudio acerca de las actividades de DoubleClick. Ya en el año 1998, un 46,8% de los usuarios de Internet visitaron un sitio de DoubleClick en Diciembre de ese año. Para Febrero del 2000, se estimó que DoubleClick había recolectado aproximadamente cien millones de perfiles[3]. Por tanto, la protección de la vida privada frente a tales compañías es de interés público.

[2] http://www.fas.org/irp/cia/product/ig_deutch.html (visitado por última vez el 25 de Agosto del 2002).

[3] Jason Williams, Personalization vs. Privacy: The Great Online Cookie Debate, pág. 26, publicado el 28 de Febrero, 2000.

CAPÍTULO I

COOKIES Y LA CONSTITUCIÓN DE PERFILES

Durante los últimos años, la publicidad online ha experimentado un crecimiento proporcional al de la "*World Wide Web*". De acuerdo a un estudio realizado por la *Internet Advertising Bureau* [4], solamente en los Estados Unidos, los ingresos por concepto de publicidad en línea fueron de U$ 301 millones en 1996, para luego aumentar a U$ 5.62 billones en 1999, y para el 2003, se han proyectado ingresos por U$ 11.5 billones, de los cuales un 56% de los ingresos por concepto de publicidad se atribuyen a los "*banner ads*" que se destacan en las páginas web - pequeñas publicidades gráficas que aparecen en rectángulos en la parte superior o al lado del contenido primario de la página web. Hoy en día, billones de avisos publicitarios son puestos mensualmente ante la vista de los consumidores que navegan a través de la red. Empresas como *DoubleClick*, estima publicar alrededor de 1.5 billones de avisos (banner ads) por día, y alrededor de 45 billones de avisos por mes, mientras que *Engage*, la segunda empresa más grande en publicidad en la internet, publica aproximadamente 8.6 billones de avisos por mes. Generalmente, estos avisos no son seleccionados y distribuidos por los sitios web que uno visita, sino por una empresa publicitaria que administra y provee publicidad gráfica para un sinnúmero de páginas web. *DoubleClick*, y *Engage*, dos de las empresas publicitarias más grandes en la Red, estiman que más de la mitad de los usuarios online han visto un *banner ads* proporcionado por ellos [5].

Generalmente, estas empresas publicitarias no solamente proporcionan avisos, sino que también recolectan datos respecto de los consumidores que ven estos avisos. Como ha escrito Paul Schwartz [6], una vez conectado a Internet nuestra computadora deja de ser una “amiga silenciosa y leal” y se transforma en una grabadora que traiciona nuestros secretos. La transformación a la que alude Schwartz ocurre, en el caso de la utilización de cookies y web bugs. [7], los cuales rastrean los hábitos del usuario en Internet. La cookie transmite información al servidor que la instaló y que, en general, sólo puede ser leída por ese servidor. Los web bugs son pequeños archivos de imágenes invisibles a simple vista contenidas en una página web. Los web bugs funcionan enviando información relativa al

[4] Ver Internet Advertising Revenues, en http://www.iab.net (Internet Advertising Bureau).

[5] Ver http://www.doubleclick.com; http://www.engage.com/press_room/ .

[6] Protección de Datos y Privacidad, Cap. 13: Privacidad y Comercio Electrónico, pág. 267.

[7] Un *web bug o escucha web* es un gráfico GIF transparente dentro de una página web o dentro de un correo electrónico del mismo color del fondo y con un tamaño de 1x1 píxeles. Normalmente, al igual que ocurre con las cookies, son puestas ahí por terceras partes para entresacar información acerca de los lectores de esas páginas o correos. La información recabada sobre el visitante gracias a esta imagen incluye entre otros datos la dirección IP de su ordenador, el URL de la imagen, que codifica los datos que serán enviados desde la página web visitada al sitio recolector de información, la fecha y hora en que fue vista la imagen, el tipo y versión de navegador del internauta, su sistema operativo, idioma e incluso valores de cookies si es que no están deshabilitadas. Ver http://www.iec.csic.es/criptonomicon/susurros/susurros32.html

usuario (frecuentemente es la dirección IP del computador del usuario, el URL (ver nota 8) de la página donde está situado el web bug y el tiempo que la página fue navegada por el usuario) al servidor que los puso en esa página. Así, las cookies quedan instaladas en el disco duro del computador, y los web bugs permanecen estacionados en la página web.

Respecto al tipo de información que puede ser reunido por las compañías publicitarias, encontramos: la información entregada por los consumidores a la página web visitada; el tiempo y duración de la visita al sitio; los buscadores introducidos en un motor de búsqueda; compras online; y la página web que el consumidor visitó anteriormente a la página actual que está siendo vigilada. Toda esta información puede ser obtenida sin que el consumidor cliquée sobre los *banner ads*.

La información recopilada por las compañías publicitarias es frecuentemente, pero no siempre, anónima; por ejemplo, los perfiles reunidos muchas veces están ligados a un número de identificación que corresponde al cookie que se encuentra inserto en el disco duro del usuario. Estos datos generalmente se conocen como "información identificable no personal"[8]. Sin embargo, en otros casos los perfiles obtenidos a través del rastreo de actividades online, coincide con información personal identificable o IPI. Los datos personales identificables son datos que pueden ser vinculados a individuos específicos, y puede incluir información como nombre, teléfono, correo electrónico, cédula de identidad, etc. Esta recolección de información personal puede hacerse de dos maneras cuando el consumidor se identifica a un sitio web en que exista *banner ads* de la empresa publicitaria. En primer lugar, el sitio web al cual se proveyó la información personal, puede a su vez traspasar los datos a una compañía publicitaria. O en segundo lugar, la IPI puede ser incorporada a un URL[9], el cual es automáticamente transmitido a la empresa publicitaria a través de un cookie.

Una vez reunido, los datos personales pueden ser analizados y combinados con datos demográficos y psicográficos pertenecientes a terceras partes, o con información recopilada directamente de consumidores a través de encuestas o formularios. Estos datos ampliados permiten que la compañía publicitaria realice una serie de conjeturas acerca de los intereses y preferencias de cada consumidor. El resultado final es un perfil detallado que intenta predecir los gustos, necesidades y hábitos de compra de un consumidor individual, permitiendo así que los sistemas computacionales de la empresa publicitaria realice funciones de distribución de propaganda dirigida a los intereses específicos de los consumidores en línea en materia de segundos.

Estos perfiles creados por la empresa publicitaria pueden ser extremadamente detallados. Una cookie inserta por la compañía puede localizar al consumidor en cualquier sitio web donde la compañía preste sus servicios. Por lo tanto, la recolección de datos puede darse a lo largo de la Red y respecto de páginas completamente inconexas entre si. Además, en lo temporal, las cookies relacionadas a banner ads son incansables, ya que pueden rastrear a los consumidores durante un extenso lapso de tiempo, anotando cada vez que el usuario se conecte a Internet. Finalmente, cuando la información reunida es combinada con la base de datos de terceras partes, estos perfiles pueden llegar a incluir

[8] Non-personally identifiable information o non-PII.

[9] **URL**. Localizador Uniforme de recursos (*Uniform Resorce Locator*). Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El url esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.unam.mx) más el directorio y el archivo referido.

cientos de clasificaciones distintas, como por ejemplo, en el caso de la compañía *Engage*, donde sus perfiles llegan a tener 800 categorías distintas de intereses.

A pesar de los constantes y casi perpetuos rastreos para la constitución de perfiles, estas actividades son invisibles para la mayoría de los consumidores. Todo lo que ve un usuario de internet es la página web que visita, y los avisos publicitarios que parecieran formar parte integral del sitio; mientras tanto, las cookies son insertadas desapercibidamente en el computador del usuario[10]. A no ser que el sitio web que visita el usuario posea una política mediante el cual da aviso al consumidor acerca de la presencia de la compañía publicitaria y su recolección de datos, el consumidor estará completamente inadvertido que sus acciones en línea están siendo rastreadas.

A) EJEMPLO ILUSTRATIVO DE LA CONSTITUCIÓN DE PERFILES

Un consumidor en línea, Diego Rojas, visita una página web que vende productos deportivos. Realiza un click en la página en busca de bolsas de golf. mientras tanto, aparece un *banner ads*, el cual ignora. Este aviso es puesto por *USAad Network*. Más tarde visita un sitio para turismo e ingresa en el buscador la palabra "Hawai". *USAad Network* también proporciona avisos en este sitio, y Diego observa un aviso respecto al arriendo de autos. Diego luego visita una librería online y busca libros que traten acerca de las mejores canchas de golf en el mundo. *USAad network* proporciona avisos en esta página web también. Una semana más tarde, Diego visita su sitio de noticias favorito, y avista un aviso acerca de promociones de vacaciones de golf en Hawai. Interesado, él cliquea sobre el aviso, el cual es proporcionado por *USAad Network*. Más tarde, Diego empieza a sospechar si el aviso era pura coincidencia, y si no lo era, cómo fue que apareció.

Durante la primera visita que Diego realiza al sitio de bienes deportivos, su browser automáticamente enviará cierta información al sitio, el cual necesita para poder comunicarse con el computador de Diego: su tipo de browser y sistema operativo; el idioma aceptado por el browser; y la dirección de internet del computador. El servidor del sitio de bienes deportivos responde transmitiendo los códigos HTTP y HTML de la página web, lo cual permite que en el computador de Diego aparezca la página solicitada[11]

En el código HTML que el browser de Diego recibe del sitio de productos deportivos, viene escondido un vínculo al sitio de *USAad Network*, el cual permite que aparezca un aviso en el espacio reservado para publicidad en el sitio web de artículos deportivos. El browser de Diego es estimulado automáticamente para que envíe mediante un HTTP cierta información a *USAad Network* relativa al tipo de browser y su sistema operativo; el idioma o idiomas aceptado por el browser; la dirección de la página de artículos deportivos; y el número de identificación e información reunida en la cookie de *USAad* inserta en el computador de Diego. De acuerdo a esta información, *USAad Network* colocará un aviso en

[10] La mayoría de los *browsers* pueden ser configurados para que notifiquen acerca del hecho que una cookie está siendo enviado al computador del usuario, dándole la posibilidad de rechazar la cookie. Sin embargo, la configuración preestablecida de los browsers permite la inserción de la cookie sin notificación alguna.

[11] Hypertext Transfer Protocol (el protocolo que permite la comunicación entre el browser y el servidor); y Hypertext Markup Language (el código e idioma con que se transmite el contenido de la página).

el espacio reservado para publicidad en la página principal del sitio de productos deportivos. Este aviso parecerá como si fuera parte integral del sitio web. Si todavía no existe una cookie de *USAad* implantada en el computador de Diego, *USAad* se encargará se poner una cookie con un identificador único en el disco duro. De esta manera, Diego no tiene idea alguna acerca del hecho de que se esté colocando una cookie en su computador, a no ser que tuviese configurado su browser para que le notificara el hecho. Por tanto, cuando Diego cliquea en la página sobre bolsas de golf, la dirección URL de la página revela su contenido, pero al mismo tiempo lo transmite a *USAad* mediante la cookie.

Luego que Diego deja la página de productos deportivos, y visita el sitio de viajes, donde también presta servicios *USAad*, un proceso similar toma lugar. El código HTML para el sitio de viaje contendrá un vínculo invisible a *USAad* que requerirá el envío de un aviso que formará parte de la página web de la agencia de viajes. Debido a que el requerimiento revela que el sitio solicitante es de viajes, *USAad* envía un aviso relacionado al arriendo de autos. *USAad* también conocerá el número de identificación de su cookie en el computador de Diego. A medida que Diego navega a través de la página de viajes, *USAad* chequea su cookie y modifica el perfil asociado a ella, agregando elementos basados en las actividades de Diego. Cuando Diego ingresa la palabra Hawai en el buscador, su búsqueda es transmitida a *USAad* a través del URL utilizado por la página web de la agencia para localizar la información que Diego requiere, y al mismo tiempo, el término ingresado es asociado con los otros datos recolectados por la cookie en el disco duro de Diego. *USAad* también registrará los avisos mostrados a Diego, y si éste cliqueó en ellos.

Este proceso es repetido nuevamente cuando Diego visita la librería virtual. Debido a que este sitio también posee avisos de *USAad*, también reconocerá a Diego con motivo del cookie con su número de identificación. Asimismo, *USAad* podrá rastrear qué libros Diego revisa, aunque no los compre. El hecho que Diego examine libros relacionados a canchas de golf también es incorporado a su perfil.

En síntesis, basado en los hábitos de internet de Diego, *USAad* puede deducir que Diego es un golfista que está interesado en viajar algún día a Hawai, y puede ser que esté interesado en unas vacaciones con golf. Por ende, una semana más tarde, cuando Diego visita su página web favorita de noticias, a la cual *USAad* también presta servicios, la cookie en su computador es identificado, razón por la cual se publica en ese sitio un aviso con una oferta de vacaciones de golf en Hawai. El aviso atrae su atención, y consiguientemente hace click sobre el.

B) BENEFICIOS E INQUIETUDES SURGIDOS DE LOS PERFILES Y LA PRIVACIDAD

Beneficios

Las cookies son utilizadas para varios otros fines distintos a los perfiles realizados por terceras partes publicitarias, muchos de los cuales aportan beneficios significativos para los consumidores. Por ejemplo, los sitios web muchas veces solicitan a los usuarios sus nombres y claves correspondientes al momento de comprar o previamente a que cierto tipo de contenidos sean entregados. Las cookies pueden registrar estos nombres y claves para que los consumidores no tengan que ingresarlos cada vez que visiten la página. Otra función de las cookies está relacionado con los sitios web que permiten a los consumidores acumular productos en un carro de compras electrónico, mientras deciden realizar o no la compra; las cookies permiten que el sitio recuerde qué productos están acumulados en el carro como efecto de visitas anteriores. Las cookies además pueden ser usadas por sitios web para ofrecer páginas personalizadas u otros contenidos personalizados según

los intereses individuales de los consumidores. Los comerciantes online también pueden usar cookies para rastrear las compras de sus compradores, y de este modo ofrecerles nuevos productos u ofertas en las cuales puedan estar interesados en razón de ser clientes frecuentes. Finalmente, mediante el uso de cookies los dueños de páginas comerciales pueden revisar constantemente el diseño y delineación de sus páginas web con el objeto de hacerlas más atractivas y eficientes para los navegantes.

En relación al uso de cookies y otras tecnologías para la creación de programas publicitarios, también tiene su lado positivo tanto para consumidores como los comerciantes. De acuerdo a la *Asociación de Publicistas Nacionales* [12], la publicidad dirigida a individuos determinados permite que los consumidores reciban ofertas e información relativa a productos y servicios que realmente les interesa. La publicidad dirigida también puede mejorar las experiencias del usuario en internet, simplemente al asegurar que el usuario no sea bombardeado repetidamente con los mismos avisos. Los comerciantes también se benefician de la publicidad dirigida, ya que evitan gastar recursos en publicidad que llega a consumidores que no están interesados en sus productos.

Adicionalmente, la publicidad dirigida en línea ayuda a subsidiar los contenidos gratis que existen en Internet. Al hacer publicidad más efectiva mediante el uso de perfiles, esto permite que los sitios web cobren más por publicidad puesta en sus páginas. Estos ingresos por concepto de publicidad contribuyen a subsidiar sus operaciones, haciendo posible que se ofrezcan contenidos gratis en sus sitios web, en vez de estar cobrando para tener acceso a la página.

Por último, el uso de perfiles en la publicidad online puede ser utilizado para la creación de nuevos productos y servicios. Por ejemplo, la gente de negocio puede usar los perfiles para realizar un estudio de mercado, y determinar la demanda que existe por ciertos productos y servicios, o puede ayudar a las PYMES, mediante un ingreso al mercado con menores costos, al publicitar únicamente a consumidores que tengan un verdadero interés en sus productos o servicios.

En resumen, la publicidad dirigida trae consigo numerosos beneficios tanto para los comerciantes como para los consumidores de internet.

Inquietudes por el uso de Perfiles

A pesar de los beneficios que trae consigo la publicidad dirigida, hay mucha inquietud relacionada con ciertas prácticas desleales en el uso de perfiles. Principalmente, ha habido reclamos concernientes a ciertas compañías de publicidad que realizan rastreos encubiertos de consumidores *online*, y respecto de la recolección de vastas cantidades de datos sin el conocimiento o consentimiento de los usuarios de internet. La *Federal Trade Comisión* (de ahora en adelante FTC o Comisión) ha constatado la falta de *opciones* que los publicistas dan a los consumidores respecto al uso y propagación de la información personal recopilada. Tal como lo manifestó un usuario en una encuestas realizada por la FTC respecto a la configuración de perfiles, "las prácticas actuales socavan las expectativas de privacidad de los individuos, fundamentalmente al convertir la experiencia de navegar en internet y buscar información en forma anónima, en una donde cada movimiento de la persona es registrada".

La más significativa y consistente inquietud de los usuarios en relación a la constitución de perfiles, es que son efectuadas sin el conocimiento de los consumidores. La presencia e identidad de la compañía publicitaria en un sitio determinado, la introducción del cookie en

[12] ANA - Association of National Advertisers.

el computador del usuario, el rastrear los movimientos del consumidor, y los avisos dirigidos son hechos invisibles en la mayoría de los casos. Esta afirmación es muy cierta, ya que hay sólo dos maneras para que el usuario sepa lo que ocurre en un sitio determinado. La primera es que la página web que utiliza los servicios publicitarios publique el hecho en sus políticas de privacidad. Desafortunadamente, es muy raro que esto ocurra. En una encuesta aleatoria realizada por la *Comisión* a los sitios más visitados en la red, aunque un 57% permitía que terceros insertaran cookies, solamente un 22% de estos sitios informa acerca de las cookies o de la recolección de datos en sus políticas de privacidad[13]. La segunda manera es configurar el browser para que le notifique al usuario la posibilidad de aceptar o rechazar la cookie[14]. Una encuesta llevada a cabo por la revista *Business Week* en Marzo del 2000 revela que solamente un 40% de los usuarios ha escuchado sobre cookies, y de ese porcentaje, sólo un 75% tienen un concepto básico de lo que son[15].

Otra de las grandes inquietudes manifestadas por los usuarios de internet es el amplio uso del monitoreo de los hábitos de las personas en línea. También es desconocido por los usuarios que las empresas publicitarias de Internet, rastrean a individuos a lo largo de la red y durante períodos indefinidos de tiempo. El resultado de ello son perfiles mucho más completos que los que pudiese recopilar un sitio web por si mismo.

Otra inquietud expresada, es que a medida que los consumidores empiecen a enterarse acerca del monitoreo de sus actividades en internet, el temor a ser rastreado desalentará el uso de funciones muy importantes de la red, las cuales se ejercen gracias al manto del anonimato. De acuerdo al *Centro para Democracia y Tecnología*[16], "el anonimato que entrega internet a los individuos la ha convertido en una excelente fuente para aquellos que buscan información. Particularmente respecto de aquella información controversial, en materias como el sexo, sexualidad o la salud, y respecto de cuestiones como el sida, la depresión y el aborto; por ende, la facultad que entrega para acceder a información sin el riesgo de revelar la identidad es indispensable".

Finalmente, ciertos consumidores opinaron que la publicidad dirigida es inherentemente injusta y engañosa. Su argumento es que este tipo de publicidad es manipuladora, ya que se aprovecha de la ingenuidad de los usuarios para minar la autonomía e intimidad de los individuos en internet. De acuerdo a una encuesta realizada por IBM en 1999 en relación a la privacidad en línea, un 92% de los encuestados manifestaron su preocupación frente a las amenazas en contra de su intimidad personal al usar internet, y un 80% de los consumidores expresaron haber perdido todo control sobre cómo su información personal está siendo recolectada y utilizada por las compañías.

[13] La descripción y metodología del estudio realizado por la FTC, se encuentra en su informe del 2000 al Congreso de los EEUU.

[14] Para poder configurar esta opción en Internet Explorer 6.0, el usuario debe cliquear en el menú "Tools", y seleccionar "Internet Options"; luego cliquear en la etiqueta "Security", y elegir la opción "Custom Level"; luego bajar hasta llegar a la opción "cookies" y seleccionar "Prompt".

[15] Ver BUSINESS WEEK ONLINE, BUSINESS WEEK/HARRIS POLL: A GROWING THREAT, www.businessweek.com/2000/00_12/b3673010.htm

[16] Comentario del Center for Democracy and Technology (CDT).

Si analizamos la encuesta realizada por *Business Week*[17], podemos apreciar que un 89% de los consumidores online no están cómodos con la idea de que sus hábitos de navegación y de compras están siendo reducidos a perfiles que se vinculan a sus verdaderos nombres e identidades; y si a ese perfil le están agregando datos personales como sus ingresos, cédula de identidad, información crediticia y su estado de salud, un 95% expresa su disconformidad. Los consumidores incluso se oponen a perfiles que contengan datos con información no personal: un 63% de los consumidores expresa no sentirse cómodos con que sus acciones en línea sean rastreadas, aunque dichos datos no se relacionen con sus identidades reales. Finalmente, un contundente 91% indica que no está cómodo con que los sitios web compartan la información de modo que puedan ser rastreados a lo largo de la red.

Muchos consumidores indicaron que sus inquietudes acerca de la recolección de datos personales y el uso de perfiles se verían disminuidos, si los sitios informaran claramente acerca de qué información podría ser recolectada y para qué usos se ocuparía, y si además les dieran la posibilidad (opt-out) de excluirse de la recopilación o el uso particular de sus datos personales. Una encuesta llevada acabo por "*Privacy & American Business*" les explicó a los usuarios de internet que para que las empresas publicitarias realizasen publicidad dirigida, las compañías necesitarían datos personales acerca del consumidor. A los usuarios luego se les preguntó si estarían dispuestos a proveer información: (1) que describiera sus intereses; (2) permitiendo el uso de la información cuando visitasen las páginas web; (3) permitiendo el uso de información durante sus compras en línea; (4) permitiendo el uso de información durante sus compras *offline*; (5) permitiendo la combinación de datos relacionados con las compras *online* y *offline*. Si las compañías entonces se comprometieran a publicar cómo utilizarían la información personal del consumidor y se les diera la opción de excluirse de cualquier uso que no aprobaran, una mayoría de los usuarios se mostró dispuestos a entregar información personal. Por tanto, sujetos a los principios de *notificación* y *opción*[18], un 68% de los encuestados mostraba disposición para describir sus intereses; un 58% estaban dispuestos a permitir el uso de sus datos al visitar un sitio web; un 51% permitía el uso de información durante las compras *online*; un 53% estaban dispuestos a permitir el uso de datos para la compra *offline*; y un 52% estaban dispuestos a autorizar la combinación de información relativa a compras en línea y *offline*.

Aunque esta encuesta indique que con la aplicación de opción y notificación, muchos de los consumidores estarían dispuestos a permitir el uso de su información personal para fines de publicidad dirigida; sin embargo, las estadísticas también demuestran que muchos consumidores no están dispuestos a permitir el uso de perfiles, sin importar haya o no notificación y opción. Entre un 32% y 49% de los usuarios encuestados manifestaron no tener la disposición para permitir el uso de información personal, aunque se les informara acerca del uso de los datos y se les diera la opción de *opt-out* respecto de lo que no aprobaran.

Los usuarios de internet también expresaron mayoritariamente su rechazo a la propagación onerosa de sus datos personales. Un 92% dijo que no se sentían cómodos con que sitios web compartieran información personal con otras organizaciones, y un 93%

[17] Encuesta realizada por la revista Business Week en Marzo del 2000, para determinar el punto de vista de la opinión pública respecto al uso de perfiles.

[18] Ver los principios fundamentales para la protección de datos personales contemplados en el Informe del año 1998 de la FTC al Congreso de los EEUU.

rechazaba la idea de la venta de información. Un 88% de los consumidores dijo que les gustaría que las páginas web les solicitaran la autorización cada vez que quisieran compartir los datos personales con terceros.

Para concluir, es necesario recalcar que los intereses de privacidad de los consumidores de internet, son también intereses para los empresarios de la red. El mercado electrónico solamente logrará su potencial máximo cuando los usuarios se sientan más seguros para navegar y comprar en línea. Esta seguridad podrá lograrse, si los consumidores saben que: (1) están siendo notificados que en ese instante se está recabando información, quién lo está recolectando, qué información se recaba, y cómo pretende usarse; (2) ellos tienen la opción para elegir si sus datos son recolectados, cómo son usados, y con quién se comparte dicha información.

CAPÍTULO II

EL MARCO NORMATIVO EN LOS ESTADOS UNIDOS

A) A NIVEL CONSTITUCIONAL

De acuerdo a la causa **Olmstead v. United States** [19], se estableció que el derecho a estar solo, "es el más comprensivo de los derechos, y el más valorado por los hombres civilizados". A diferencia de los estados europeos, los Estados Unidos jamás ha tratado a la intimidad como una garantía fundamental. Al contrario, la explotación de información personal para fines comerciales es una actividad tradicional y muy desarrollada en el mercado anglosajón. Por ende, a medida que las empresas norteamericanas penetran en los mercados extranjeros, su recolección y explotación de datos personales constantemente va aumentando.

La Constitución de los Estados Unidos no contempla el derecho a la intimidad en forma expresa, y por ende, sus ciudadanos no gozan de un derecho federal explícito a la privacidad. Sin embargo, la Corte Suprema de los EE.UU. ha sostenido que "*la Constitución garantiza el derecho a la privacidad personal en ciertas áreas o materias*" [20]. Sin embargo, esta afirmación fue hecha en el marco de un caso donde se disputaba el derecho de una mujer al aborto. Hasta hoy, la Corte Suprema no ha extendido el derecho a la privacidad de la información personal de un individuo.

Específicamente, si analizamos la jurisprudencia de la Corte Suprema respecto de la primera enmienda, no se ha encontrado ningún caso donde se trate la privacidad en la información; y en cuanto a la cuarta enmienda, la doctrina no ha podido relacionar la invasión de la privacidad a las nuevas tecnologías. La Corte Suprema de los Estados Unidos ha determinado que la Constitución, a través de la primera y cuarta enmienda, implícitamente garantiza ciertos ámbitos del derecho a la privacidad.

En el caso particular de la primera enmienda, esta se ha concentrado en garantizar el derecho de las personas para realizar ciertas decisiones personales sin la interferencia del gobierno [21]. Por ejemplo, en la causa **Griswold vs. Connecticut**, la Corte sostuvo que la opción de usar anticonceptivos era un asunto esencialmente personal, por lo que el gobierno no estaba autorizado para intervenir. Sin embargo, hasta el momento la Corte Suprema todavía no ha fallado un asunto donde se establezca que el derecho a la privacidad limite los actos de gobierno con relación a la recopilación de datos personales.

Por otro lado, la cuarta enmienda que protege a las personas contra pesquisas arbitrarias, tiene un mayor nivel de desarrollo en cuanto a la protección de datos personales

[19] Olmstead v. United States, 277 U.S. 439, 478 (1927).

[20] Roe v. Wade, 410 U.S. 113, 152 (1973).

[21] El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohíba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agrarios (primera enmienda).

[22]. En la causa **United States vs. Katz**, la Corte falló que la cuarta enmienda protege toda información que la persona subjetivamente considera que se respetará como información privada, siempre que dicha expectativa sea razonable para la sociedad. Si embargo, esta **razonable expectativa** de privacidad no garantiza que los datos personales sean protegidos completamente. La mayoría de las veces los individuos por diversos motivos llegan a compartir la información privilegiada. Una vez compartida, aunque sea por un lapso de tiempo breve, la persona ya no podrá alegar que poseía una razonable expectativa de privacidad. Para aclarar el concepto, analicemos el fallo de una corte de Virginia en la causa **United States vs. Hambrick**, donde se aplica la razonable expectativa a un asunto de internet. La Corte falló que el usuario de internet no tenía una razonable expectativa de privacidad respecto de la información personal que su proveedor de internet reveló a los investigadores gubernamentales. La Corte basó su fallo en el hecho de que la información fue entregada voluntariamente al proveedor desde un principio, por lo que no podía considerarse como información esencialmente privada.

Sin embargo, la cuarta enmienda que protege a las personas de pesquisas y aprehensiones arbitrarias, puede ser usado para proteger a los individuos de la recolección ilegal de información por parte del gobierno. En el caso **Katz vs. United States**[23], la Corte Suprema reconoció que la cuarta enmienda protege a las personas y no a lugares. Lo que una persona concientemente enseñe a público, aunque sea en su hogar u oficina, no puede ser objeto de protección por parte de la cuarta enmienda. A su vez, una cosa que expresamente la persona busca mantener como privada, aunque esté en un área de acceso al público, puede estar amparado constitucionalmente. No obstante esta garantía, ciertos sectores privados se las han ingeniado para usufructuar de información recolectada por el Estado, vulnerando los datos personales de los individuos. Así por ejemplo, respecto a la emisión de permisos de conducir en el Estado de Texas, la ley estatal permite la venta de bases de datos de base sobre licencias pero prohíbe a su vez su publicación en Internet. Pese a ello, personas como Vincent Cate publican la información en Internet[24]. Una vez más surge la cuestión acerca de la falta de uniformidad en la legislación internacional respecto a Internet. Mientras en Texas existe leyes de privacidad que prohíben la publicación de información relativa a licencias de conducir en la red, no puede impedir que individuos como Cate, quien presta sus servicios en Anguilla, una dependencia británica, vulnere las leyes tejanas sobre privacidad.

Por tanto, la cuarta enmienda evita que el Estado y los gobiernos federales lleven a cabo allanamientos o detenciones arbitrarias e ilegales. Sin embargo, hoy en día se le ha permitido al gobierno federal de los Estados Unidos desarrollar programas informáticos como “Carnívoro”. Este software implementado por el FBI tiene como objetivo establecer un sistema de monitoreo que intervenga los correos electrónicos nacionales, lo cual es sinónimo de pesquisas no autorizadas de los e-mails. Las autoridades del FBI, por su lado, argumentan que el sistema de Carnívoro no tiene la capacidad para supervigilar el correo de una persona determinada, pero sí contribuye enormemente a la capacidad federal para

[22] El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas (cuarta enmienda).

[23] 389 U.S. 347 (1967).

[24] Steward Taggart, Fast, Cheap and Out of Control, The Industry Standard, Aug. 14, 2000, at 178, 181.

combatir el cibercrimen en una sociedad que tecnológicamente avanza muy rápido[25]. Sin embargo, aquellos que se oponen a *Carnívoro* por aumentar la capacidad gubernamental para realizar pesquisas arbitrarias, fundamentan su postura con ejemplos como es el caso de proveedores de servicios de internet (PSI). Si un PSI como AOL permitiera que el FBI instalara Carnívoro en sus servidores, el PSI pasaría a convertirse en un instrumento del Estado. "Aunque el PSI sea una puerta para que los consumidores accedan a la internet", la mayoría de ellos ignora el hecho que el PSI tiene la facultad para "ver virtualmente todo" lo que un consumidor hace. El problema radica en que los PSI normalmente no aclaran suficientemente este punto en sus cláusulas de privacidad con sus clientes. Tal como lo afirma Emily Whitfield, miembro de la *American Civil Liberties Union* con sede en Washington: "sin importar cuanto un PSI proteja la privacidad de sus consumidores, si el gobierno permite que el FBI utilice el sistema Carnívoro en los proveedores de servicios de internet, el correo electrónico de cada uno será un libro abierto"[26].

Por ende, mientras algunas partes de la constitución promueven la protección de datos personales, otras partes limitan esta garantía. La principal piedra de tope que restringe la protección de información privada es la Primera Enmienda, y el derecho a la libertad de expresión. La intimidad de los individuos no puede ser protegida, si antes afectar en cierto modo la libertad de expresión. En otras palabras, la privacidad de información es la antítesis de la finalidad de la primera enmienda: proteger el libre flujo de información.

Por lo tanto, aunque la Corte Suprema haya fallado ciertos casos de invasión a la privacidad a través de la primera y cuarta enmienda, estos derechos les ofrecen poca protección a los usuarios de internet. Los derechos a la privacidad anteriormente citados no se aplican a la información traspasada libremente, aunque sea para un fin legítimo, y que posteriormente sea utilizada en forma ilícita. Por ello, estas garantías constitucionales solamente protegen a los individuos frente a los actos de gobierno, y no respecto de particulares u organizaciones privadas.

B) LEGISLACIÓN APLICABLE

En el caso de la legislación reguladora de la intimidad en los Estados Unidos, no existe un conjunto de leyes coherentes, sino leyes de parche que se han creado a medida que fueron surgiendo nuevas tecnologías que atentaban contra la privacidad de los individuos. Un claro ejemplo de esta tendencia histórica de improvisar frente a las coyunturas del momento, fue el testimonio dado ante el Congreso por el juez Bork frente a su nominación para la Corte Suprema. Durante su testimonio, algunos parlamentarios cuestionaron su moral debido a la información que poseían respecto a los tipos de videos que usualmente arrendaba. Estos datos personales se obtuvieron legalmente, ya que simplemente se solicitó a su tienda de videos local la lista de los videos que había arrendado en el último tiempo. Ante los reclamos

[25] FBI Internet Surveillance: The Need For A Natural Rights Application Of The Fourth Amendment To Insure Internet Privacy, por Catherine M. Barrett, Capítulo III Analyzing Carnivore Under Existing Federal Law.

[26] http://zdnet.com.com/2100-11-528747.html?legacy=zdnn; "Privacy Paranoia: Can EarthLink Cash In?" por Stephanie Olsen (8 de Marzo, 2001).

de la opinión pública frente a tal problema, el Congreso aprobó la Ley de Protección a la Privacidad de Videos de 1988[27].

En síntesis, el Congreso norteamericano ha aprobado una serie de leyes en el ámbito de la protección de datos personales, pero sin una estructura definida e interrelacionada. Así, podemos citar la “Electronic Communications Privacy Act”; el “Federal Records Act”; “Cable Communications Privacy Act”; “Telephone Communications Protection Act”; “Freedom of Information Act”; “Children’s Online Privacy Protection Act”; "Gramm-Leach-Biley Act", etc.

Entre las leyes mencionadas, una de las más completas en protección de datos personales en Internet es la “Electronic Communications Privacy Act” de 1986 o ECPA. La ECPA afecta significativamente la privacidad en la red, ya que prohíbe a los proveedores de internet el revelar los contenidos de las comunicaciones electrónicas a terceros. Sin embargo, esta ley contiene una excepción que permite al recibidor de un mensaje divulgar su contenido. Esta excepción tiene una amplia interpretación, ya que los operadores de sitios web a los cuales sus usuarios les han comunicado información personal, se han acogido a esta norma, ya que también les conferiría la naturaleza de recibidores, y por tanto, tendrían la facultad de hacer lo que quisiesen con la información. Por ende, esta legislación ofrece nula protección en el caso de información otorgada libremente a los operadores de páginas web, quienes podrán transferir los datos personales a terceros interesados.

Debido a que los proveedores de páginas web y los comerciantes electrónicos han sido incapaces o no han tenido la voluntad de implementar la autorregulación de la industria en forma eficiente y coordinada con respeto a la intimidad, han surgido varias voces apoyando la dictación de un estatuto legal federal cohesionado que garantice la protección de datos personales en la internet. Además de lo anterior, la Directiva sobre Privacidad de la Unión Europea ha inhibido la expansión de algunos comerciantes electrónicos estadounidenses, ya que sus políticas de privacidad son insuficientes para la legislación europea. Esta situación hace necesaria la creación de un cuerpo legal federal coherente que establezca parámetros mínimos para la protección de la intimidad de los consumidores en internet, y que a su vez ofrezca mecanismos para la solución de conflictos jurisdiccionales. Semejante texto legal ya existe en los EE.UU. pero solamente regula la situación de menores de trece años. Es la llamada "*Children's Online Privacy Protection Act*" o COPPA, ley que regula cuándo y cuánta información personal se puede reunir de menores de edad.

Promulgada en Octubre de 1998, COPPA ha logrado disminuir significativamente los temores de muchos padres, y al mismo tiempo le ha complicado la existencia a un sinnúmero de operadores de internet. Esta ley requiere que los operadores de sitios web dirigidos a menores de edad publiquen en sus respectivas páginas acerca de qué información es recolectada y para qué propósito. COPPA además exige que los operadores de estás páginas obtengan la autorización expresa de los padres antes de poder reunir o utilizar dicha información. Otra obligación que impone este estatuto, es el deber que tienen los operadores de otorgar a los apoderados la posibilidad de revisar los datos que los sitios han recolectado de sus hijos, y la prohibición de mantener o usar posteriormente esta información. Finalmente, COPPA requiere que los operadores mantengan mecanismos que garanticen la protección de la confidencialidad, seguridad e integridad de la información reunida de los menores. En cuanto al ente administrativo encargado de fiscalizar y sancionar a aquellos que violen las disposiciones de COPPA, dicha tarea recayó en la Comisión Federal de Comercio (FTC) a partir de Abril del 2000.

[27] Video Privacy Protection Act of 1988.

La *Gramm-Leach-Biley Act*, conocida también como la *Ley de Modernización de los Servicios Financieros*, fue aprobada en 1999 para facilitar las transacciones entre bancos, instituciones financieras, y compañías de seguro, principalmente a través del intercambio de información. Su *título V* establece que toda institución financiera debe dar a conocer a sus afiliados su política de privacidad, tanto respecto de sus clientes como de terceros. Además le presenta a los clientes la oportunidad de rehusarse a compartir sus datos personales con terceros no afiliados (opt-out). Esta última disposición tiene por objeto proteger la intimidad de aquellos afiliados a instituciones financieras que realizan parte de sus operaciones online. Sin embargo, como sucede con otros estatutos legales que regulan datos personales, esta ley carece de medios de imposición sobre los operadores de internet.

C) ACCIONES DEL EJECUTIVO Y AUTORREGULACIÓN

La política desarrollada por los EE.UU. en cuanto a la protección de datos ha sido la autorregulación por parte de la industria. A comienzo de los ochenta, la administración Reagan recomendó a los empresarios adoptar voluntariamente las directrices de la OECD respecto a los datos personales[28]. Aunque casi 200 compañías acogieron estas directrices, poco hicieron para incorporarlas a sus operaciones diarias. Frente a ello, durante las últimas dos décadas, las administraciones presidenciales de los EE.UU. han mantenido una actitud principalmente pasiva en cuanto al tema. Por ello, se habla de que el gobierno se inclinó por una autorregulación de la industria de la informática en el área de la privacidad, en vez de que interviniera el gobierno concretamente. Lo más próximo a una regulación estricta a nivel nacional por parte del gobierno federal en cuanto a la protección de datos personales, fue el requerimiento a la FTC para que realizara un estudio de cuatro años en relación a la privacidad de los consumidores *online*. Por ende, a la FTC se le encomendó la misión de investigar si la industria había realizado esfuerzos suficientes como para frenar los abusos contra los datos personales, y como consecuencia de ello, si era necesario que el Congreso entrara a legislar.

Al iniciar esta investigación de cuatro años, la FTC se propuso como meta "incentivar y facilitar la autorregulación efectiva como el método más apropiado para proteger la privacidad de los consumidores on-line"[29]. Después de una exhaustivo análisis de alrededor de mil cuatrocientas páginas web, la FTC concluyó que los esfuerzos de la industria para incentivar la implementación voluntaria de las medidas más básicas para la protección de consumidores ha sido deficiente. A pesar de ello, la FTC no aconsejó al Congreso que llevara a cabo ninguna legislación concreta respecto al asunto. Solamente enumeró una serie de directivas para que fueran implementadas por la industria de Internet[30]. En razón de ello, los administradores de páginas web que publicasen cláusulas a favor de la privacidad de sus clientes, podían ser hechos responsables si sus políticas de

[28] Organization for Economic Cooperation and Development, **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 de Septiembre de 1980.**

[29] Informe al Congreso sobre la Privacidad On Line por la FTC (Junio 1998); http://www.ftc.gov/reports/privacy3/priv-23a.pdf .

[30] Las cuatro proposiciones hechas por la FTC se encuentran en http:// www.ftc.gov/opa/1998/9807/privacyh.htm (21 de Julio de 1998), en el párrafo cuarto.

privacidad no eran materializadas. Como consecuencia de estas directrices, se produjo un incentivo inverso para el acogimiento de cláusulas de privacidad, ya que las compañías se veían más favorecidas si no publicaban estipulación alguna en favor de sus clientes.

En 1999, la Comisión Federal de Comercio nuevamente sugirió al Congreso que no legislara en relación a la privacidad *on-line*, favoreciendo la idea de la autorregulación. Sin embargo, el año 2000, la posición de la FTC tomó un giro de ciento ochenta grados, ya que sostuvo que la autorregulación por si sola no era capaz de proteger adecuadamente la privacidad de los consumidores *on-line*, debido a que existía una falta de protección generalizada entre los sitios de internet. Se realizó un estudio aleatorio con treinta y nueve mil visitas a distintas páginas web, y se pudo comprobar que solamente el veinte por ciento de los sitios había puesto en práctica las cuatro directrices sugeridas por la FTC. La Comisión también visitó los cien sitios comerciales más populares de los Estados Unidos donde pudo constatar que sólo un 42% de ellos cumplía cabalmente con las cuatro directrices[31]. Por primera vez en tres años, la Comisión recomendó al Congreso que legislara para "asegurar la adecuada protección de la privacidad de los consumidores online".

D) ORGANISMOS CONTROLADORES – LA FTC

Debido a los vacíos legales que surgen a partir de la legislación ineficiente en materia de privacidad en Internet, el Congreso de los EE.UU. le ha delegado ciertas facultades reguladores a la *Federal Trade Commision* o FTC. Lamentablemente, la FTC no fue creada para dicho propósito, y además no posee la autoridad suficiente como para regular efectivamente los conflictos en materia de intimidad en la red. Más encima, la FTC tiene una serie de funciones anexas a la internet (relacionadas al comercio y la protección del consumidor), por lo que se ve imposibilitada de destinar recursos suficientes para la protección de la privacidad de los individuos en la internet.

La FTC tiene como misión promocionar el funcionamiento eficiente del mercado a través de una debida protección de los consumidores de actos o tratos injustos o engañosos, y de aumentar las alternativas para los consumidores mediante la promoción de una amplia competencia. Por ende, el mandato legal primordial de la *Comisión* (o FTC) es la aplicación de la Ley de la Comisión Federal de Comercio o *Federal Trade Comisión Act* (tratada de ahora en adelante como FTCA), la cual prohíbe métodos desleales de competencia, y actos o prácticas injustas o engañosas que afecten el comercio. Con la excepción de ciertas actividades e industrias, la FTCA le otorga a la *Comisión* amplios poderes de fiscalización y aplicación del derecho sobre entidades que se dedican a la actividad del comercio. Por lo tanto, el comercio en la Internet se encuentra dentro de los marcos legales que regula este estatuto.

Debido a la repetida práctica de recolección en línea y uso de información de consumidores, incluyendo la vigilancia de los hábitos personales de los *browsers*, se ha producido una manifiesta inseguridad para los usuarios de la Internet. Este fenómeno no es nuevo; desde 1997 se han realizado encuestas que demuestran la molestia de los navegantes virtuales en relación a la recopilación de datos personales dentro del mercado

[31] Ver "FTC recomienda al Congreso Ley para la Protección de la Privacidad de Consumidores Online", 22 de Mayo 2000, http:// www.ftc.gov/opa/2000/05/privacy2k.htm

online[32]. Frente a ello, la *Comisión* se propuso como meta realizar un análisis acabado del mercado virtual, y de sus pros y contras.

A pesar de su rol limitado en el ámbito de Internet y la intimidad, es necesario destacar los logros positivos que obtuvo la FTC. En primer lugar, la FTC tuvo cierto éxito al intervenir en el caso de **Geocities**. En 1998, la FTC interpuso una demanda en contra de Geocities, un popular portal de internet, por contravenir una cláusula donde expresamente le prometía a sus usuarios adoptar voluntariamente una política de privacidad, donde se comprometía a una serie de condiciones, como por ejemplo, que notificaría a todos sus miembros respecto de qué información poseía, e incluso permitiendo que ellos borrasen toda información personal de su base de datos[33]. Sin embargo, se tuvieron que acumular grandes cantidades de prueba que demostraran los fraudes e ilícitos para que finalmente pudiera intervenir la FTC. Nuevamente, esto demuestra la ineficiencia del sistema frente a los atropellos a la privacidad en la red.

El Congreso también le confirió a la FTC la obligación de presentar anualmente un informe acerca del estado presente de la privacidad en la internet, y por consiguiente, recomendarle al Congreso en que dirección debiese legislar. Fue así como en 1998, la FTC le recomendó al Congreso que legislara respecto a la protección de la privacidad de los menores en línea. En 1999, el informe de la FTC reveló que el 66% de los sitios web publicaron algún tipo de aviso que prevenía acerca de la utilización de información personal, aunque muy pocos sitios proporcionaron a los usuarios algún tipo de protección de sus datos personales. Esto se debe a que la FTC ha optado por un sistema en que la industria de Internet se autorregule, en vez de imponer normas reguladoras más estrictas. Para el año 2000, la FTC realizó otra encuesta, en base a la cual se concluyó que la privacidad en línea todavía constituía un enorme desafío para las autoridades, y que a su vez, los intentos de autorregulación por parte de la industria no habían sido suficientes, por lo que se le recomendaba al Congreso legislar con el objeto de establecer un nivel básico de protección de los datos personales respecto de los sitios web dedicados al comercio.

E) ANÁLISIS DEL INFORME ANUAL AL CONGRESO DE 1998

En 1998, la *Comisión* resumió sus conclusiones finales concernientes a la recolección, uso y difusión de datos personales en su informe sobre privacidad en línea al Congreso. Este informe destacó primordialmente una serie de principios respecto a prácticas legítimas para el comercio online, las cuales han sido recogidas y desarrolladas por instituciones estatales en los EEUU., Canadá y Europa desde 1973, cuando el Departamento de Salud, Educación y Bienestar de los Estados Unidos publicó un informe sobre la protección de privacidad en la era de recolección de datos, registros, computadores, y los derechos de los ciudadanos. El Informe de 1998 identificó los principios fundamentales para la protección

[32] Estos datos fueron publicados en el informe anual de la FTC en 1998, ante el Congreso de los EEUU, Capítulo II, B, Nº2, "*Privacy Concerns*".

[33] Discurso de Debra Valentine respecto a la Privacidad en la Internet, Feb. del 2000 (http://www.ftc.gov/speeches/other/dvsantaclaraspeech.htm).

de datos personales, encontrados comúnmente en decretos gubernamentales, directrices, y códigos modelos. Estos principios son:

1.- Notificación: los recolectores de datos deben informar acerca de sus prácticas recopilatorias antes de poder recolectar información personal de los consumidores;

2.- Opción: los usuarios de internet deben tener la posibilidad de elegir cómo la información reunida va a ser utilizada más allá del propósito para la cual fue entregada;

3.- Acceso: los navegantes de internet deben ser capaces de revisar, completar y corregir la información reunida respecto a ellos;

4.- Seguridad: los recolectores de datos deben tomar los procedimientos necesarios para asegurar que la información recopilada de los consumidores sea exacta y segura contra usos no autorizados.

El informe también reconocía la facultad *sancionadora* de la *Comisión*, es decir, el uso de un mecanismo efectivo para imponer sanciones por el incumplimiento de la obligación de abstenerse de llevar a cabo prácticas comerciales desleales, con el objeto de garantizar la privacidad en línea.

En el informe de 1998, se hace un detallado análisis de las prácticas recopilatorias de los sitios web y del existente sistema de autorregulación por parte de la industria, y en base a los principios de prácticas justas en la reunión de datos personales, se concluyó que la autorregulación todavía era deficiente. La Comisión nada dijo sobre la necesidad de legislar sobre la protección de la privacidad en línea de los consumidores, y en cambio, optó por presionar a que la industria acelerara programas de autorregulación más efectivos. Un año después, la Comisión nuevamente recomendó a la industria de Internet que implementara la autorregulación, y que pusiera en práctica los principios generales para la protección de datos personales[34]. Por fin en el año 2000, en su informe al Congreso, la FTC concluyó que a pesar de los logros significativos hechos en materia de autorregulación, igualmente los esfuerzos de la industria en su conjunto fueron insuficientes. Por ende, la mayoría de la FTC recomendó al Congreso que se legislara para asegurar una debida protección de la privacidad online.

F) JURISPRUDENCIA

1) Doubleclick

A continuación entraremos a analizar la jurisprudencia anglosajona más relevante en materia de las cookies y su vínculo a la protección de datos personales. Dado que no existe estatuto federal que específicamente regule la recolección y diseminación de información íntima a través de la internet (excepto en el caso de menores de trece años), algunas partes han optado por demandar en base a ciertas leyes comerciales federales, leyes estatales de protección al consumidor y ciertas leyes por falsa publicidad.

El caso más emblemático en relación a la protección de datos personales, llegó a conocimiento público el 10 de Febrero del año 2000. La empresa ***DoubleClick*** , el mayor proveedor de publicidad en Internet en el mundo, anticipó al mercado su fusión

[34] Informe al Congreso de 1999, "Self-Regulation and Online Privacy: a Report to Congress".

con *Abacus-Direct*, compañía que poseía una amplia base de datos de sus clientes. Ante ello, el Centro Informativo de Privacidad Electrónica (EPIC) interpuso un reclamo contra DoubleClick ante la FTC. EPIC argumentaba que los intereses comprometidos era la protección de la privacidad de los individuos, y que esta fusión se traducía en una amenaza de un mal uso de información personal, ya que permitiría que terceros obtuviesen información relativa a empleos, seguros, créditos, servicios médicos, etc. EPIC también sostuvo que DoubleClick se caracterizaba por constante y drásticamente cambiar sus políticas de privacidad, por lo que en un inicio le garantizaba a sus usuarios que la compañía no tendría conocimiento alguno de los datos personales de aquellas personas que visitasen las páginas web asociados a la empresa. Sin embargo, posteriormente la política de la compañía fue modificada, permitiendo que se identificase el servidor y el tipo de browser de un usuario, lo cual era divulgado con terceras partes involucradas en el ámbito de la publicidad.

Luego de su fusión con Abacus Direct, DoubleClick anunció que empezaría a asociar los nombres y direcciones de la lista de clientes de Abacus con los perfiles de los usuarios de DoubleClick, a través de un código inserto en sus cookies. DoubleClick aseguraba publicar en sus páginas web avisos en el cual les notificaba a los usuarios acerca del proceso para recopilar información. Sin embargo, EPIC sostenía que la mayoría de los navegantes de internet que recibían cookies de DoubleClick y que también tenían su información personal en la base de datos de Abacus, nunca visitaban las páginas que informaban acerca de las prácticas de la compañía para recolectar información y acerca del procedimiento para optar salir del proceso de recopilación de datos. Por lo tanto, EPIC fundó su demanda en la sección 5, letra (a) de la Ley de la FTC, la cual prohibía prácticas injustas o engañosas en el comercio. Específicamente, EPIC alegaba que: (a) *DoubleClick* publicó que cualquier información personal recolectada de sus usuarios, se mantendría en el presente y futuro como confidencial; (b) DoubleClick pretendía cotejar la información "confidencial" de sus usuarios con los nombres, direcciones y el registro histórico de consumo contenida en la base de datos de *Abacus*. La demanda también ponía énfasis en que la conducta de DoubleClick causaba daños substanciales a los consumidores; por ejemplo, la invasión de su privacidad, la cual no podía ser razonablemente evadido por los consumidores (no había una real posibilidad de *opt-out*), ni existían beneficios para los consumidores que contrapesaran estos perjuicios. Por lo tanto, EPIC demandó reparación mediante las siguientes pretensiones: (a) la destrucción de la base de datos de los usuarios, respecto de los cuales DoubleClick había prometido absoluta confidencialidad; (b) una investigación de la información reunida por DoubleClick y de sus prácticas publicitarias; (c) se le dictamine a DoubleClick que obtenga el consentimiento expreso de sus usuarios respecto del cual se pretenda crear un registro personal; (d) indemnizaciones equivalentes al 50% de las ganancias logradas como consecuencia de las prácticas ilegítimas invocadas en la demanda; (e) un mandato permanente para que DoubleClick respete y no contravenga las disposiciones contempladas en la Ley de la FTC; compensaciones por los daños causados a los consumidores como efecto de las violaciones de DoubleClick.

En otra instancia, a finales de Enero de 2000, **Harriet Judnick**, en representación del interés público del Estado de California, interpuso una acción civil en contra de DoubleClick Inc. en la Corte Superior de California. La demandante pretendía indemnización por perjuicios sobre la base del uso de tecnología para identificar personalmente los usuarios de Internet, específicamente mediante la utilización de cookies. La acción también buscaba que se fijaran mecanismos por la Corte para la destrucción de todos los registros que poseían datos personales y de los correos electrónicos que fuesen utilizados para la publicidad de productos comerciales. La demandante argumentaba que DoubleClick había

incurrido en prácticas comerciales ilegales, engañosas y fraudulentas que invadían y perjudicaban el derecho a la intimidad.

Dentro de la misma semana, el defensor público para Michigan, Jennifer Granholm anunció su intención de demandar a DoubleClick por infracción a la Ley de Protección al Consumidor de Michigan. Granholm basó su acusación sobre los mismos hechos que alegaba EPIC en relación a las prácticas desleales para la recopilación de datos y su fusión con Abacus Direct, enfatizando las constantes modificaciones que la compañía realizaba a su política de privacidad. Granholn además afirmaba que el método de *opt-out* utilizado por DoubleClick, no le proporcionaba a los consumidores una notificación que explicara suficientemente la opción que tenían respecto a aceptar o no la recolección y posterior uso de sus datos personales. Además, Granholm alegó otras infracciones, como la implantación de cookies en los computadores de los usuarios era un hecho desconocido y no autorizado por ellos; que la promesa de DoubleClick respecto a la confidencialidad de la información era falsa y confusa; y finalmente que DoubleClick falló en comunicar a los consumidores su propósito de utilizar los datos que recolectaba y de obtener el consentimiento expreso de los usuarios antes de recopilar la información. Cada una de estas prácticas constituía una infracción a la Ley de Protección al Consumidor de Michigan.

Paralelamente a las acciones anteriores, *Harriet Judnick* entabló otra acción en contra de DoubleClick y doscientos de sus empresas asociadas en el Estado de California. Judnick basó su demanda sobre los mismos hechos relativos a la recolección y revelación de datos personales de usuarios de internet, y exigió indemnización de perjuicios por invasión a la intimidad, y por publicidad engañosa. La primera pretensión de Judnick estableció que los usuarios de internet tienen una razonable expectativa de privacidad al visitar una página web o al comprar productos online, y que Doubleclick y sus asociados no proporcionaron avisos o publicidad suficiente relativo a sus prácticas de recolección de datos, ni adecuadas medidas para impedir la recopilación de datos personales, ni medidas suficientes para recuperar información personal ya reunida, ni la adecuada protección ante la amenaza de revelación de información a terceros no asociados. Dichas conductas, de acuerdo a la parte demandante, constituía una violación al derecho a la intimidad garantizado en la Constitución de California, como también prácticas ilegales, fraudulentas y engañosas frente al Código de Comercio y Profesiones de California[35]. Judnick también alegó que DoubleClick y sus asociados eran responsables de publicidad engañosa, ya que en sus políticas de privacidad vía internet garantizaban al público que ninguna información sería reunida, retenida o desclasificada a terceros, pero que por el contrario, la información era recolectada si los usuarios no realizaban una serie de pasos para lograr un *opt-out*, a pesar de la razonable expectativa que tales prácticas no se estaban llevando acabo. Concretamente, la parte demandante tenía como pretensión que DoubleClick y sus asociados dejaran de utilizar cookies y tecnología semejante para identificar usuarios sin que previamente obtuviesen el consentimiento expreso del afectado; que DoubleClick destruyese todos los perfiles de los usuarios contenidos en la base de datos reunidos sin consentimiento; y exigir de DoubleClick y de sus asociados que declaren públicamente que la compañía obtuvo información personal que identificaba a los usuarios sin su consentimiento, y que en adelante la compañía solamente recopilaría la información con el consentimiento expreso de los usuarios.

En Marzo del 2000, DoubleClick entró a negociar con las partes demandantes anteriormente mencionadas. Como resultado de ello*, DoubleClick* anunció que echaba pie atrás en su propósito de fusionar su base de datos con perfiles de usuarios online con la

[35] Ver art I, sección 1 de la Constitución de California, y el "*California Business and Professions Code*".

información para identificación personal contenida en la base de datos de *Abacus Direct*. Un año más tarde, la Corte para el Distrito Sur de Nueva York rechazó una demanda contra DoubleClick, sobre la base de que los demandantes no fueron capaces de establecer una pretensión fundada. Específicamente, la corte consideró que la parte demandante fue incapaz de probar que DoubleClick tuvo acceso no autorizado a los computadores personales a través del uso de cookies. La corte consideró que DoubleClick obtuvo acceso legítimo a los computadores de los usuarios a través de las páginas web de sus asociados publicitarios. Finalmente, la corte falló que la información recogida por DoubleClick era similar en naturaleza a la recopilada de otros consumidores, y que por ello, el valor de la información no representaba daño alguno para los usuarios de Internet o un enriquecimiento ilegítimo para los recolectores.

2) Geocities, Inc.

En Mayo de 1998, la Comisión Federal de Comercio inició una investigación respecto de una página web por el mal uso de información personal identificable (IPI) de sus usuarios. Tras la investigación, Geocities reconoció que sus prácticas violaban varias de las disposiciones contempladas en la ley de la FTC, y aceptó una serie de condiciones impuestas por la FTC en un acuerdo suscrito entre las partes. La FTC en un inicio había alegado que el sitio web de Geocities, el cual ofrecía servicios gratis de internet, violaba sus propias políticas de privacidad al vender información de sus clientes a terceras partes, los cuales la utilizaban para publicidad en general, aunque se garantizaba a los usuarios que los datos solamente serían distribuidos si el consumidor expresamente lo consentía. También la FTC inició acciones en contra de Geocities por falsa publicidad, ya que publicitaban que la información personal recolectada de menores era recogida y archivada por ellos, cuando en realidad era recopilada por terceros vía la página web de Geocities.

La FTC y Geocities firmaron un acuerdo donde la Comisión incluyó un conjunto de directrices y políticas, con el objeto de establecer una serie de precedentes para el resto de las compañías de internet. La FTC utilizó este caso para demostrar a la opinión pública su voluntad para demandar a todos aquellos sitios que no cumplieran cabalmente con lo establecido en sus políticas de privacidad. La más llamativa de las estipulaciones contenidas en el *Acuerdo* exigía que Geocities proveyera a los "consumidores avisos claros y sobresalientes" respecto a las prácticas de la compañía para la recolección y posterior uso de información personal identificable. Este aviso que demanda la FTC, debía contener como mínimo: qué información estaba siendo recolectada; sus posibles usos e información relativa a la posibilidad que tienen los usuarios para lograr acceso a los datos; y los métodos a través de los cuales pueden remover directamente dicha información de la base de datos de Geocities; y el procedimiento mediante el cual los consumidores puedan eliminar IPI de la base de datos de Geocities.

Para verificar el cumplimiento de las directrices impuestas por la FTC, se le otorgó un plazo de sesenta días a Geocities para que evacuara un informe escrito, "señalando en detalle la manera y forma con que dieron cumplimiento a las demandas de la FTC". Finalmente, la última estipulación del acuerdo establecía que el acuerdo suscrito no se extinguía sino hasta el 5 de Febrero del 2019, o "hasta veinte años después a la más reciente fecha en que los Estados Unidos o la FTC entablara una acción en una corte federal alegando una violación del acuerdo".

Además, conforme a la Sección V de la ley de la FTC (ley en que se basaron las acciones entabladas contra Geocities), Geocities podía ser multado con hasta U$10 mil

por cada violación al acuerdo suscrito por las partes. Con el objeto de determinar las multas y sanciones contempladas en la ley, cada violación en si es considerada una ofensa separada; excepto en el caso en que se produzca una violación permanente y continua del Acuerdo, la cual se medirá por días, constituyendo cada día un agravio por separado.

3) Toysmart.com, Inc.

En Mayo del 2000, *Toysmart.com*, empresa de propiedad de *Walt Disney Company*, dejó de recibir pedidos en su página web que se dedicaba a juegos educativos para niños. El 9 de Junio del mismo año, acreedores de *Toysmart.com* solicitaron a los tribunales su declaración de quiebra. La solicitud fue acogida por la corte de quiebra el 26 de Junio del 2000. Mientras tanto, *Toysmart.com* empezó a publicar avisos en periódicos buscando posibles compradores para la adquisición de sus activos, incluyendo su base de datos con su lista de clientes. En esa época, la base de datos de *Toysmart.com* contenía perfiles personales y de familias, además de datos sobre tarjetas de créditos correspondientes a unos 250 mil consumidores que habían visitado la página desde sus inicios.

En respuesta a la oferta pública de la base de datos de *Toysmart.com*, la FTC interpuso una demanda en Julio del 2000 en la Corte del Distrito de Massachussets, con la pretensión de impedir que la quebrada empresa vendiese datos con información de sus consumidores. La FTC alegaba que la venta hecha por Toysmart.com constituía una violación a sus políticas de privacidad, y posiblemente a las leyes sobre privacidad de los Estados Unidos [36]. Por ende, el propósito de la FTC tras la acción legal interpuesta, era desbaratar los planes de la compañía por vender los datos personales.

La demanda interpuesta por la FTC sostenía que la compañía infringía la Sección 5 de la Ley de la FTC, al pretender vender sus listas y perfiles de sus consumidores, incluyendo información personal contribuida por menores a través del sitio web de *Toysmart.com*. Casi inmediatamente, la FTC aprobó un Acuerdo Estipulado conteniendo un Mandato Definitivo con los dueños de *Toysmart.com*, *Walt Disney Company*. La estipulación permitía que la compañía vendiese su lista de consumidores en un procedimiento de quiebra, "siempre que el comprador se adhiriera a la política de privacidad previa de Toysmart.com en orden a salvaguardar la lista". Las cláusulas del acuerdo requerían que Toysmart.com vendiese la lista en un paquete conjunto, incluyendo el sitio web, y a un "vendedor calificado" en un mercado similar, según lo determinado por la jueza Kenner. El acuerdo también exigía que la compañía eliminase miles de registros recopilados en violación a la Ley de Protección a la Privacidad de Menores en Línea de 1998.

Tras interponer el Mandato Definitivo, treinta y nueve fiscales de estado le solicitaron al magistrado Kenner que suspendiera la venta porque violaba directamente las leyes de privacidad de cada uno de sus estados. Más encima, la compañía de internet *TrustE* que certifica protecciones de privacidad en el comercio electrónico, acompañó documentos en el juicio contra *Toysmart.com* con el objeto de impedir la venta de la lista de consumidores [37]. La magistrado Kenner manifestó ciertas dudas con respecto al acuerdo suscrito entre

[36] Ver nota de prensa publicada por la FTC el 21 de Julio del 2000, "FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations"; http://www.ftc.gov/opa/2000/07/toysmart2.htm

[37] TrustE es una empresa de Internet que entrega su certificado de calidad a aquellos sitios web y compañías de comercio electrónico que cumplan con ciertos códigos de prácticas leales de información *online*. TrustE también exige de las compañías a las cuales entrega su sello de calidad, que se sometan a sus programas de monitoreo en línea de privacidad.

Disney, *Toysmart.com* y la FTC, por lo que el 18 de Agosto del 2000, dictó sentencia. En ella, la jueza Kenner dejó de lado ciertas condiciones contenidas en la propuesta de venta de *Toysmart.com*; por ejemplo, que la lista de clientes sólo fuese vendida en un paquete a alguien perteneciente a la industria; y que el acuerdo suscrito con el órgano regulador, solamente podía ser aplicado una vez que existiera un comprador concreto para los activos de *Toysmart.com*.

Finalmente, en la parte resolutiva de la sentencia, la corte declaró estar "perpleja" frente al por qué la FTC se encontraba entablando una demanda contra Toysmart.com, dado que no tenía la calidad de acreedor dentro del procedimiento de quiebra. Consiguientemente, la corte requirió a la Comisión que redactara un informe dentro del plazo de 15 días con el objeto de aclarar cuál era su razonamiento jurídico tras la acción entablada.

4) RealNetworks, Inc.

RealNetworks es una empresa de software con residencia en el estado de Washington, la cual otorga en forma gratuita a los usuarios de internet el uso de dos de sus productos: RealPlayer y RealJukebox. Estos productos permiten a los usuarios ver y escuchar audio y videos disponibles en la Internet, como también bajar, grabar, y tocar música. Antes de poder instalar y utilizar este software, el usuario debe registrarse en la página web de la compañía; esto involucra revelar información personal, incluyendo el nombre y correo electrónico. Después de registrarse, *RealNetwork*s autoriza bajar el software, pero asignándole también un vínculo, relacionando así la copia del programa con el nombre y correo del usuario. En relación a esta práctica, *RealNetworks* argumenta que la recolección de información no es anónima, pero sí privada.

El 1 de Noviembre de 1999, el diario "New York Times" publicó un reportaje donde afirmaba que *RealNetworks* estaba rastreando los hábitos de individuos utilizando su software. Frente a ello, tres usuarios de estos programas (Michael Lieschke, Robert Jackson y Todd Simon) demandaron a RealNetworks de comunicarse con computadores personales que tenían instalados RealPlayer y RealJukebox para obtener información acerca de las costumbres del usuario en internet.

Para poder usar productos de RealNetworks, a los demandantes se les solicitó aceptar los términos de acuerdo impuestos en el sitio web de la compañía. Este convenio aceptado por los demandantes, sin embargo, no hacía mención alguna respecto a la recopilación de datos personales, implantación de cookies, o el posible uso de los datos reunidos, por parte de *RealNetworks*. El convenio meramente informaba a los usuarios que el software de *RealNetworks* se comunicaría en forma automática con el usuario sólo para ciertos fines como actualizaciones, nuevas versiones, parches, etc., y que el usuario sería notificado en cualquiera de estos eventos. Por lo tanto, los demandantes basaron su acción en la recolección y posterior uso de sus datos personales sin su conocimiento.

CAPÍTULO III

EL MARCO NORMATIVO EN LA UNIÓN EUROPEA

A) ANTECEDENTES HISTÓRICOS

A continuación realizaremos un breve análisis de la Directiva de la Unión Europea concerniente a la privacidad, la cual obligaba a los estados miembros uniformar sus legislaciones conforme a la directiva para el 24 de Octubre de 1998[38]. Dicha directiva trata la privacidad de datos como un derecho humano fundamental, a través del cual se protege datos personales que son recolectados por los gobiernos o para fines comerciales. Queda fuera de la esfera de esta directiva los datos recolectados para fines personales o del hogar.

A diferencia de los Estados Unidos, las naciones europeas y particularmente la Unión Europea (UE.), con relación a la protección de datos personales, han legislado en forma sistemática, ya sea en el ámbito de los particulares o lo público, como también se han creado organismos gubernamentales que específicamente se dedican a implementar estos estatutos legales.

En cuanto a los intentos legislativos individuales de cada nación para la protección de datos personales, podemos afirmar que no se trata de hechos recientes. Ya a mediados del s. XIX, varias naciones europeas establecieron leyes que protegían a los individuos de que se publicase sin su consentimiento información de su persona. Países como Suecia, Francia y Alemania fueron pioneros en aprobar leyes para la protección de datos durante el siglo XX. Por ejemplo, en 1973 Suecia aprueba su primera ley nacional sobre la protección de datos, conocida como el Estatuto Sueco de Datos Bancarios. Este estatuto impedía que empresas recolectaran datos de los ciudadanos suecos, a no ser que previamente fuesen autorizados por autoridades gubernamentales. También fue creado una entidad gubernamental, el Consejo Nacional de Inspección de Datos, la cual otorgaba licencias para la recolección de datos, y que a su vez fiscalizaba que el procedimiento de recolección de datos se hiciese en conformidad al Estatuto mencionado anteriormente. Otra función del Consejo Nacional de Inspección de Datos o *DataInspektionen*, era regular el flujo saliente de información personalizada del país, para lo cual se requería su autorización expresa. Por ende, Suecia utilizaba un proceso de licencias para restringir la salida de información a países con poca regulación jurídica en relación a la protección de datos[39].

En 1978, Francia aprobó la Ley de Protección de Datos. Bajo dicha ley, tanto las agencias gubernamentales como entidades privadas requerían que obtuviesen el consentimiento expreso de las personas para poder consiguientemente procesar sus datos personales. Es la "*Commission Nationale de L'informatique et Des Liberté*" la encargada de hacer cumplir esta ley a través de reclamos, el establecimiento de reglamentos, realizar auditorias, etc.

[38] Directriz Nº 95/46/EC (24 de Octubre de 1995), http://europa.eu.int/

[39] Ver "Transborder Data Flows" por Tom Ogaranko, Capítulo 3; en www.compusmart.ab.ca/ogaranko/tdf/tdftoc.htm

En cuanto al caso específico de Alemania, como consecuencia de las fuertes violaciones a la privacidad de los ciudadanos durante el régimen Nazi, la Corte Constitucional Federal Alemana criticó fuertemente que el gobierno mantuviera un inventario de datos personales, las cuales obtuvo a través de un censo confidencial. En 1970, el estado alemán de Hessen fue el primero en aprobar una ley de protección de datos la cual se aplicaba solamente al sector público. Más adelante, el propio Estado Federal Alemán utilizó la ley de Hessen como modelo para su Ley de Protección de Datos Personales y su Mal uso en el Procesamiento de Datos, pero a diferencia del estatuto legal de Hessen, el estatuto federal se aplicaba tanto al sector público como privado, y contemplaba tanto la recolección manual como automatizada de datos.

El primer intento de protección de datos a nivel europeo se produjo a mediados de los setenta, y culminó con la **Directiva 95/46/EC** de la Unión Europea sobre la "*Protección de Individuos con respecto al Procesamiento de Datos Personales y la Libre Circulación de tales Datos*", de 24 de Octubre de 1995.

Dos fueron los organismos encargados de fundar las bases para la Directiva sobre Protección de Datos: la OECD (Organization for Economic Cooperation and Development) y el Consejo Europeo. En 1980, la OECD fijó una serie de directrices internacionales para la protección de la privacidad de los consumidores con relación a transacciones internacionales. Estas directrices incluían tanto la recolección manual y automatizada de datos.

En cuanto al Consejo de Europa y su influencia en la protección de datos, en 1981 dio nacimiento a al Convenio 108 sobre la Protección de Individuos con respecto al Procesamiento Automático de Datos Personales. Mientras las directivas de la OECD eran mucho más amplias que el Convenio 108 en cuanto a la materia que regulaban, no eran vinculantes para los países que las ratificaban, por lo que la primera norma era más eficiente en materia de protección.

Más adelante fue la Comunidad Económica Europea (CEE) y luego la Unión Europea, los que tomaron la responsabilidad de continuar con la labor iniciada por el Consejo de Europa con relación a la protección de datos. Esto debido a que la protección de datos es considerada una actividad comercial, y por tanto, está incluido dentro de la competencia del mercado único europeo. Con la dictación de la Directiva de Protección de Datos del '95, se pretendía fundamentalmente inducir a que los estados miembros "protegiesen los derechos fundamentales y las libertades de las personas naturales, y particularmente su derecho a la intimidad con respecto al procesamiento de datos personales"[40]. Dentro del proceso de integración para un mercado único, las diferencias legislativas de los estados miembros en cuanto a la protección de datos constituía un obstáculo considerable al flujo de información. Por ejemplo, las leyes restrictivas alemanas en materia de protección de datos constantemente entrarían en conflicto con otras legislaciones, si se les permitiese a las empresas alemanas intercambiar información libremente con otros estados miembros que poseen leyes más liberales, como era el caso de Italia. Al establecer una directiva única para todos los Estados Miembros en materia de protección de datos personales, se ha logrado derribar aquellas barreras nacionales que restringían el flujo de información.

Por tanto, la Directiva sobre Protección de Datos surgió como respuesta ante la amenaza de que estados miembros adoptasen leyes más estrictas que prohibiesen la transferencia de datos, como era el caso de Alemania y Francia, a otras naciones con leyes más liberales, como era el caso de Italia. Fue a través de esta amenaza de prohibición

[40] Council Directive 95/46/EC.

total de transferencia de datos, que Francia y Alemania pudieron imponer sobre otros estados miembros leyes con mayor regulación en el ámbito de protección de datos. Esto fue incorporado a la Directiva sobre Protección de Datos Personales mediante la inclusión de una cláusula de "terceras partes"[41]. Esta cláusula se refiere a la transferencia de datos personales a terceros países, es decir, a Estados no Miembros de la Unión Europea, siempre que se garantice que el respectivo país posea un adecuado nivel de protección.

B) LOS PRINCIPIOS DE PUERTO SEGURO

Similarmente al Estatuto Sueco de Datos Bancarios, la Directiva sobre Protección de Datos solamente permite la transferencia de datos personales a naciones con un adecuado nivel de protección. Sin embargo, la Directiva no define ni cita ejemplos acerca del significado de un "adecuado nivel de protección". Conjuntamente a ello, era de público conocimiento que los Estados Unidos, uno de los principales socios económicos de la Unión Europea., no poseía leyes equivalentes a la legislación europea en cuanto a la regulación de la protección de datos en el sector privado. Además, la posibilidad de prohibir cualquier transacción electrónica entre Norteamérica y la Unión Europea era inexistente. Sin embargo, si la Unión Europea certificaba que los Estados Unidos cumplía con los requerimientos para asegurar un adecuado nivel de protección como lo establece la Directiva, se estaría poniendo en duda la credibilidad de ella. Por ello, fue necesario llegar a un acuerdo entre las partes, lo cual fue conocido como los "Principios de Puerto Seguro". Estos principios fueron un compromiso convenido entre el Departamento de Comercio de los EE.UU. y la Comisión Europea para ayudar a que empresas norteamericanas no sufrieran interrupciones en las transacciones que desarrollasen con la Unión Europea o fuesen demandados por autoridades europeas por violar leyes de privacidad[42]. Estos principios entraron en aplicación el 1 de Noviembre del 2000, pero solamente para aquellos que los acogieran voluntariamente, pues jamás adquirieron el carácter de ley.

Mientras las negociaciones para los Principios de Puerto Seguro duraron dos años, una eventual falta de interés por parte de las empresas de los EE.UU. en adoptar dichos principios, puede terminar por derrumbar todo el acuerdo. Después de poco más de un año desde que entró en vigor el programa, solamente 135 compañías americanas han firmado estos principios. Defensores de la privacidad tienen la esperanza de que todo el acuerdo fracase, ya que sostienen que dicho acuerdo es una solución de parche, cuando en realidad debiese existir un tratado internacional que verse sobre la protección de datos personales. Uno de los puntos más controversiales, era la poca fiscalización de estos principios. De acuerdo a los Principios de Puerto Seguro, la empresas americanas tenían dos opciones: (a) ingresar a un programa autoregulativo de privacidad, como por ejemplo *BBB Online* o *TRUSTe*; o (b) desarrollar su propia política de privacidad conforme a los siete principios de puerto seguro. Programas autorreguladores de la intimidad, como TRUSTe, tienen la obligación de notificar a la FTC acerca de prácticas comerciales irregulares que no se sujetan a lo establecido en los Principios de Puerto Seguro. Sin embargo, ciertas autoridades reguladoras en el campo de la protección de datos anexas a la Unión Europea consideraron que ninguna de las tres principales compañías norteamericanas que

[41] ver art. 25, (1) de Directiva 95/46/EC.

[42] Ver http://www.wabco-auto.com/espanol/privacy.html

debían notificar a la FTC en caso de anomalías, cumplían cabalmente con la protección de intimidad, la resolución de disputas y fiscalización.

Por ende, la fuerte controversia surgida a partir de la creación e implementación de los Principios de Puerto Seguro, contribuye a ilustrar la dificultad que existe en convenir tratados bilaterales y multilaterales relativos a la protección de datos entre países que poseen legislaciones esencialmente antagónicas al respecto.

C) ANÁLISIS DE LA DIRECTIVA

La Directiva Europea sobre la Protección de Individuos respecto al Procesamiento de Datos Personales y la Libertad de Movimiento de Dichos Datos, fue aprobada por el Consejo de Ministros de la Unión Europea, el 24 de Octubre de 1995. Claramente, esta directiva ha sido el acuerdo internacional más importante de la última década en materia de protección de datos. Con el objeto de armonizar la legislación europea, esta directiva exigía a sus estados miembros que adaptasen sus leyes internas a la directiva. Para ello, se les otorgaba un plazo de tres años (hasta el 24 de Octubre de 1998) para que sus respectivas leyes cumpliesen con los requerimientos de la Directiva.

Su artículo primero establece que "los Estados Miembros protegerán los derechos fundamentales y las libertades de las personas naturales, y particularmente su derecho a la intimidad, con respecto al procedimiento de datos personales". Por ende, a través de esta disposición la Unión Europea le ha conferido a la privacidad de información personal la calidad de derecho humano.

La Directiva requiere que todos los Estados Miembros promulguen una ley de privacidad que recoja las siguientes políticas sobre datos personales:

1) Requisitos sobre la calidad de datos [43] **:**

a) Los datos personales deben ser procesados en forma justa y legal.

b) Limitación de Objetivo: los datos personales deben ser "recolectados para objetivos específicos, explícitos y legítimos, y posteriormente no podrán ser procesados de forma contraria a esos fines".

c) Relevante: datos personales deben ser "adecuados y relevantes para aquellos fines para los cuales están siendo recopilados y/o procesados.

d) Exactitud: datos personales deben ser "determinados, y donde sea necesario, actualizados constantemente; si algún dato es inexacto o incompleto, toda medida conducente a su eliminación o rectificación debe ser realizada para asegurar la recopilación o procesamiento de datos conforme a los objetivos.

e) Los datos personales deben mantenerse solamente durante el tiempo necesario que permita la identificación de los sujetos de acuerdo a los objetivos para los cuales son recolectados o procesados.

[43] Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union by Domingo Tan; Chapter IV Internet Data Protection Regulations in the European Union; página 7; Loyola of Los Angeles International and Comparative Law Journal; Agosto 1999.

2) Requisitos para la Legitimidad del Procesamiento de Datos [44] :

a) Consentimiento: los datos solamente pueden ser procesados si el sujeto otorga su consentimiento expreso.

b) Datos personales pueden ser procesados sólo si el procesamiento es necesario para la perfección de un contrato donde el sujeto objeto de la recopilación es parte o para trámites previos solicitados por el sujeto involucrado en el contrato.

c) Obligación legal: datos personales pueden ser procesados, si "el procesamiento es necesario para el cumplimiento de una obligación legal impuesta al controlador".

d) Intereses Vitales: datos personales pueden ser procesados si el "procesamiento es necesario para proteger los intereses vitales del sujeto relacionado a los datos".

e) Datos personales pueden ser procesados si "fuese necesario para llevar a cabo una tarea en beneficio del interés público o en el ejercicio de la autoridad oficial que recayese en el controlador o en un tercero a quien los datos fuesen revelados".

f) Intereses Legítimos: datos personales podrán ser procesados si "fuese necesario para los objetivos e intereses legítimos perseguidos por el controlador o por terceras partes a las cuales fuesen revelado los datos, excepto cuando dichos intereses son anulados por los intereses o derechos fundamentales del sujeto titular de los datos, conforme a la protección señalada en el artículo 1.

3) Derechos del Sujeto titular de los Datos:

a) Derecho de Acceso: todo sujeto titular de datos tiene el derecho de obtener del controlador "confirmación respecto a si datos relacionados con él están siendo procesados o no, e información relativa a los fines del procesamiento; las categorías de los datos involucrados; y los destinatarios o categorías de destinatarios a quienes los datos son revelados.

b) Todo titular de datos tiene el derecho para obtener del controlador "la rectificación, eliminación y bloqueo de datos, y procesamiento que no cumpla con lo establecido en la Directiva, particularmente con razón de lo incompleto o naturaleza inexacta de los datos".

c) Derecho a Impugnar: todo sujeto titular de datos tiene el derecho "a impugnar en cualquier momento sobre bases legítimas respecto al procesamiento de datos concernientes a su persona".

4) Seguridad: la Directiva requiere que los Estados Miembros "implementen medidas organizativas y técnicas apropiadas para proteger datos personales contra la destrucción accidental o ilegal, o la pérdida accidental o ilegal, y contra el acceso, revelación o alteración no autorizada". El nivel apropiado de seguridad se determina equilibrando la naturaleza misma de los datos con el riesgo asociado al procesamiento de datos.

5) Transferencia de datos Personales a Países Terceros: La Directiva no solamente regula el intercambio de datos personales entre miembros de la Unión Europea, sino también la transferencia de dichos datos a países terceros (No Unión Europea). Su **artículo 25** permite la transferencia de datos personales a países terceros, solamente si el país destinatario asegura un nivel *adecuado* de protección. Los Estados Miembros determinan si un país cumple con un adecuado nivel de protección sobre la base de aquellos factores

[44] Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union by Domingo Tan; Chapter IV Internet Data Protection Regulations in the European Union; página 7; Loyola of Los Angeles International and Comparative Law Journal; Agosto 1999

involucrados en una operación de transferencia de datos, considerando particularmente la naturaleza de los datos, la duración sugerida para su procesamiento, y la existencia en el país de leyes y medidas de seguridad concernientes a la protección de datos personales.

Sin embargo, bajo ciertas condiciones, la Directiva permite que Estados Miembros transfieran datos personales a países terceros que no cumplen con un nivel adecuado de protección. Tales transferencias pueden acontecer si una de las siguientes condiciones se lleva a cabo:

a) Consentimiento: el sujeto titular expresamente consiente a la transferencia.

b) Contrato con el sujeto titular de Datos: la transferencia es necesaria para la perfección de un contrato con el sujeto titular o para la ejecución de un contrato requerido por el sujeto titular.

c) Contrato con Tercera Parte: la transferencia es necesaria para la conclusión o la perfección de un contrato con una tercera parte en el interés del sujeto titular de los datos.

d) La transferencia es necesaria con motivo de importantes intereses públicos o para el ejercicio, establecimiento o defensa de pretensiones legales.

e) Intereses del Sujeto Titular: la transferencia es necesaria para la protección de intereses vitales del sujeto titular de los datos.

f) La transferencia es hecha en base a un registro público según las leyes y regulaciones aplicables.

En cuanto al consentimiento, el art. 7 establece que los datos personales solamente pueden ser procesados con el consentimiento del individuo o en ciertos casos de necesidad. Respecto al término “necesidad”, se refiere a que los datos personales podrán procesarse, si se cumple alguna de las cinco condiciones que expresa la norma, como por ejemplo, que sea necesario para la ejecución de un contrato o es vital para la protección de los intereses del sujeto. Otra excepción se encuentra en el art. 9 en relación a la libertad de expresión. Se permite también el procesamiento de datos personales cuando sea para el solo propósito de fines periodísticos, artísticos o de expresión literaria. Finalmente, de acuerdo al art. 8, existen ciertos datos personales que no pueden ser procesados bajo ninguna circunstancia. Es el caso de datos que manifiesten el origen racial o étnicos de una persona, sus opiniones políticas, religiosas, si pertenece a un sindicato, o acerca de su salud o sexo, etc.

El art. 6 de la directiva exige a los estados miembros que el procesamiento de datos personales sea hecho en forma justa y en sujeción a la ley, y que sirvan a objetivos específicos, explícitos y legítimos. Existe una norma imperativa de publicidad en los arts. 10 y 11, los cuales exigen a los controladores de la información personal que le revelen a los individuos afectados su identidad, es decir, que se le permita a los sujetos objeto de la recolección de sus datos personales, saber quien está recolectando sus datos y para qué fin.

Luego en el art. 12, se afirma el derecho de las personas para acceder a la información recolectada de si mismos, y para que pueden verificar si los datos personales son correctos o no. A su vez, el art. 14 confiere el derecho a las personas para objetar el procesamiento de la información cuando sirva para fines comerciales.

Respecto de los controladores de datos personales, ellos tienen la obligación y responsabilidad de asegurar la confidencialidad y seguridad de los datos. Por último, el art. 25 restringe la transferencia de datos personales fuera de la Unión Europea, a no ser que

los países terceros con que se negocie cuenten con legislación adecuada para la protección de datos personales, conforme a los estándares de la Unión Europea.

CAPÍTULO IV

NORMATIVA LEGAL CHILENA

ANALISIS DE LA LEY 19.628 “PROTECCION DE DATOS DE CARÁCTER PERSONAL”

Al realizar una transacción electrónica o visitar una página web, se entrega una gran cantidad de información relativa a las personas que participan. Estos datos al ingresar a la red, eventualmente pueden ser interceptados por terceros sin que el titular de los antecedentes lo sepa. Entonces, puede afirmarse que la "privacidad en línea es la expectativa que tienen las personas de que sus datos personales, transacciones, actividades y preferencias en la red se mantengan íntimas y no se les dé otra utilización que la convenida"[45].

Por tanto, el desarrollo de Internet ha producido un conflicto entre el derecho a la información y el derecho a la vida privada. El solo hecho de navegar en la red, y específicamente, el desarrollar operaciones comerciales o el visitar un sitio web, deja al usuario expuesto a entregar grandes cantidades de datos personales, y en muchos de los casos sin siquiera tener conocimiento de ello, y mucho menos otorgar su consentimiento.

Sin embargo, la Constitución Política de la República de Chile, en su artículo 19, nº4 "asegura a todas las personas el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia". Esta garantía fundamental se ve reforzada por la **Ley 19.628** respecto a la *Protección de Datos de carácter Personal*. Es dentro de este estatuto legal donde será analizado a continuación las cookies como herramienta informática empleada por los servidores para almacenar y recolectar datos concernientes a los usuarios de internet, y de este modo establecer perfiles determinados de las personas, hecho que para muchos constituye una clara violación al derecho constitucional a la vida privada. Para esclarecer el contexto legislativo dentro del cual se desenvuelven las cookies y la protección de datos personales, en este capítulo se pretenderá dar respuesta a las siguientes interrogantes: (A) qué datos son considerados personales y su diferencia con los llamados datos sensibles; (B) recolección y tratamiento de datos; (C) derechos de los titulares de datos; y (D) transmisión de datos a terceros.

1) DATOS PERSONALES Y DATOS SENSIBLES

En el art. 2, letra (f) de la Ley, se definen los **datos personales** como "*los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*". Por ende, dicho concepto permite incorporar una gama muy amplia de datos personales, pero como veremos más adelante, esta definición tiene un carácter residual, pues queda supeditada a aquella información que no se añada dentro del concepto global de dato sensible. Respecto a los **datos sensibles**, la Ley en su art. 2, letra (g), los define como "*aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como*

[45] Definición contemplada en "Economía Digital en Chile" (Abril 2001), Tercera Parte: Legislación, Regulación Y Gobierno Electrónico, 3. Derecho a la Privacidad vs. Derecho a la información; Cámara de Comercio de Santiago www.ccs.cl

hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual". Esta serie de causales consideradas dentro de esta disposición legal solamente tienen por objeto explicar el espíritu de la norma, es decir, qué se entiende por características físicas o morales de la persona o hechos de su vida privada, y por tanto, no poseen un carácter taxativo.

2) RECOLECCIÓN Y TRATAMIENTO DE DATOS

En cuanto a la recolección y tratamiento de *datos personales*, la Ley generalmente requiere el consentimiento expreso del titular de los datos, salvo en los siguientes casos[46]:

a) exista una disposición legal expresa que lo permita;

b) sea recolectado de fuentes de acceso público;

c) los datos sean de carácter económico, financiero, bancario o comercial, y se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes, como por ejemplo su profesión, fecha de nacimiento, etc.;

d) datos que sean necesarios para comunicaciones comerciales de respuestas directas o comercialización o venta directa de bienes o servicios;

e) datos recolectados por personas jurídicas privadas para su uso exclusivo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otro beneficio general.

Para que el consentimiento del titular sea válido, previamente se le debe informar acerca del propósito para el cual se almacenarán sus datos personales, y su posible comunicación al público; además, el consentimiento debe constar por escrito.

Conforme al art. 9 de la Ley, se establece que los datos personales solamente podrán utilizarse para los fines para los cuales fueron reunidos, salvo que fueren recolectados de fuentes accesibles al público. También el art. 7 enfatiza la excepción de datos provenientes de fuentes accesibles al público; en caso contrario, las personas involucradas en el tratamiento de datos personales deberán guardar reserva sobre los mismos. Finalmente, el art. 6 de la Ley establece que "*los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado*".

En cuanto a la recolección y tratamiento de *datos sensibles*, esta Ley generalmente lo prohíbe, a no ser que:

a) una disposición legal lo autorice;

b) el titular confiera su consentimiento expreso de forma escrita;

c) sea información necesaria para el otorgamiento de beneficios de salud para el titular.

3) DERECHOS DE LOS TITULARES DE DATOS

Respecto a los derechos conferidos al titular de los datos, contemplados en el Título II de la Ley, podemos señalar los siguientes: (a) acceso a la base de datos que contenga sus datos personales, como asimismo, acceso a cualquier información relativa a la procedencia, destinatario, propósito de almacenamiento e individualización de los terceros a quienes son

[46] Excepciones contempladas en el Título I "De la utilización de datos personales", artículo 4.

transmitidos los datos personales[47]; (b) modificación de los datos personales, en caso que se acredite que sean erróneos, inexactos, equívocos o incompletos[48]; (c) por último, sin perjuicio de las excepciones legales, podrá exigir además que se eliminen los datos, en caso que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos[49].

4) TRANSMISIÓN DE DATOS A TERCEROS

En lo relativo a la **transmisión o comunicación de datos**, de acuerdo al art.2, letra (c) de la Ley, consiste en "*dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas*". Dicha transmisión de información personal a terceros, se regula en forma semejante a las disposiciones legales concernientes a la recolección de datos, variando dependiendo si se trata de datos personales o sensibles. Respecto a estos últimos, es lógico que conforme a la naturaleza de estos datos, generalmente se prohíba su transmisión, a no ser que la ley o el titular lo autorice expresamente.

El art. 5, inc. segundo de la Ley, establece que frente a un requerimiento de transmisión de datos personales, el responsable del banco de datos deberá dejar constancia de la identidad del requirente, el motivo y el propósito del requerimiento, y el tipo de datos transmitidos. En cuanto a la confidencialidad de los datos transmitidos, el receptor sólo podrá hacer uso de ellos para los fines que motivaron la transmisión o cuando no se trate de datos personales accesibles al público en general. Finalmente, lo establecido en el art. 5 relativo a la confidencialidad y constancia de la transmisión de datos personales, no se aplicará cuando la transmisión es hecha a organizaciones internacionales en cumplimiento de tratados y convenios vigentes.

Con respecto a la transmisión de datos de carácter económico, financiero, bancario o comercial, los responsables de los bancos de datos solamente podrán transmitir a terceros dicha información cuando verse sobre obligaciones donde consten letras de cambio y pagarés protestados; cheques protestados por falta de fondos; obligaciones derivadas de mutuos hipotecarios o créditos de bancos o sociedades financieras; y aquellas obligaciones de dinero que determine el Presidente de la República mediante decreto supremo[50].

Eso sí, bajo ninguna circunstancia podrán comunicarse los datos comerciales anteriormente citados que se relacionen con una persona identificada o identificable, si transcurren cinco años desde que la respectiva obligación se hizo exigible. Tampoco podrán comunicarse dichos datos después de haber sido pagada o haberse extinguido por otro medio legal[51].

[47] Derecho de acceso contemplado en el inciso primero del art. 12 del Título II de la Ley.

[48] Derecho a modificar, contemplado en el inciso segundo del art. 12.

[49] Inciso tercero, art. 12.

[50] Ver Título III, art. 17 de la Ley.

[51] Ver Título III, art. 18 de la Ley.

B) ANALISIS DE LA LEY 19.799 "LEY SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA, Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA"

Las cookies y la protección de datos personales también puede ser analizada desde la perspectiva de la *ley 19.799 de Abril de 2002*, la cual se encarga de regular los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, y la prestación de servicios de certificación de estas firmas[52]. Las cookies como fichero de texto electrónico que se inserta en nuestros discos duros, y que recoge información para las empresas publicitarias acerca de nuestras costumbres en Internet, cabe tanto dentro del concepto de documento como de firma electrónica, contemplado en el **art. 2, letra d) y f)** respectivamente. La *ley 19.799* define al documento electrónico como *toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un medo idóneo para permitir su uso posterior*. A su vez, firma electrónica se define como *cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor*.

Por ende, desde el punto de vista de la *ley 19.799*, podemos señalar que las cookies son procesos electrónicos almacenados por un receptor con el objeto de identificar formalmente al usuario de Internet para usar posteriormente su información personal. Sin embargo, la *ley 19.799* fija ciertos límites al uso de firmas electrónicas, sobretodo en el ámbito de la privacidad de los titulares y frente al uso de sus datos personales.

Así, en primer lugar, el **art. 23, Nº2** de la presente ley, asegura a los usuarios o titulares de firmas electrónicas el derecho *a la confidencialidad en la información proporcionada a los prestadores de servicios de certificación*. Por tanto, aquellas empresas de publicidad dirigida que recolectan información personal de los usuarios de Internet a través de procesos electrónicos como las *cookies* y los *banner ads*, de acuerdo a la legislación chilena, tienen el deber de mantener reserva respecto de los datos personales que recolecten de los titulares de firmas electrónica. Además, la misma norma señala que, para que la entidad prestadora de servicios de certificación cumpla con este deber de secreto, deberá *emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada*, y asimismo, los *usuarios tendrán derecho a que se les informe acerca de las características de la prestación del servicio*.

En segundo lugar, el **art. 23, Nº6**, asegura a los usuarios o titulares de firmas electrónicas el derecho *a ser informados inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador*. Esta norma es de suma importancia, pues una de las grandes críticas que hacen los defensores de la privacidad frente al uso de *cookies* en la red, es el traspaso de información personal por parte de empresas publicitarias a terceros, sin el consentimiento de los titulares. Por lo tanto, según esta disposición, ante la posibilidad de cancelarse su inscripción en el registro de prestadores, se les otorga a los usuarios de Internet la facultad de oponerse al traspaso de sus datos personales a terceros receptores.

[52] Art. 1, Ley 19.799

En síntesis, podemos sostener que la *Ley 19.799* sobre firmas electrónicas, aplicándola de manera analógica al caso de las *cookies* y los *banner ads*, otorga ciertas garantías a los titulares de medios electrónicos frente a los constantes abusos de empresas publicitarias que muchas veces recolectan información electrónica y la transfieren a terceros sin el consentimiento de los usuarios. Por tanto, esta ley asegura a los titulares de medios electrónicos, el derecho a la confidencialidad y el derecho a ser informados con el fin de hacer valer su oposición al traspaso a terceros, y así evitar tratos arbitrarios y abusivos en el mundo de las cookies.

CAPÍTULO V

DOCTRINA IBEROAMERICANA

A) DOCTRINA CHILENA

De acuerdo a información entregada por la agencia *The Associated Press* [53] (de ahora en adelante AP), el gobierno estadounidense compró a una empresa de ese país, *ChoicePoint*, el acceso a bases de datos sobre cientos de millones de habitantes de diez países latinoamericanos, aparentemente sin su consentimiento, con el objeto que una serie de agencias federales rastreen a extranjeros ubicados en los Estados Unidos.

Esta empresa ubicada en los suburbios de Atlanta, reunió la información en el extranjero y la vendió en los últimos 18 meses a autoridades estadounidenses de una treintena de agencias, incluyendo el Servicio de Inmigración, que la utiliza para arrestar a indocumentados. ChoicePoint (www.choicepointinc.com) es la mayor empresa dedicada a comercializar detalles personales de extranjeros. Desde 2001, la compañía vende bases de datos completas sobre ciudadanos latinoamericanos.

Para Robert Ellis Smith, abogado que examina las actividades de las agencias de crédito como editor de la revista "*Privacy Journal*", "este caso constituye la globalización de un problema muy desafortunado del consumidor estadounidense". En declaraciones a la AP, Smith agregó que los gobiernos latinoamericanos deben proteger a sus ciudadanos con leyes de protección a la vida privada similares a los estatutos europeos, que prohíben comprar información personal en gran escala.

A pesar de que Chile no figura entre los diez países mencionados por AP, ya existe la posibilidad de obtener nuestros datos personales a través del sitio web del Servicio Electoral. Salvo los servicios públicos que por ley deben observar confidencialidad o reserva sobre los antecedentes personales de los chilenos, como el Servicio de Impuestos Internos y el INE, el abogado Renato Jijena agrega que "los restantes –en especial el Servicio Electoral- comercializan sus bases de datos en forma abierta". El Servicio Electoral vende el padrón de los chilenos en menos de $ 17 millones. La base de datos contiene nombre completo, profesión, fecha de nacimiento, domicilio y cédula de identidad. En el sitio web de este servicio (www.servel.cl), basta cliquear en "*Biblioteca*" y luego en "*Productos a la venta*" para tener acceso a los datos personales de la mayoría de los chilenos.

Para Jijena, esto significa negociar "la identidad de un chileno", ya que no existe un estatuto jurídico adecuado que regule esta anomalía legal. "Cuando se intentó legislar en materia de procesamiento de datos personales, mediante la vigente 19.628, se inventó una categoría *amplísima* de *fuentes públicas de información*, esto es, todas las que no sean de acceso secreto o reservado". "Se prescindió de la exigencia de autorización previa de los titulares para su procesamiento y no se prohibió la transferencia internacional de los datos" [54].

[53] Protección de la vida Privada: EE.UU. compra datos de latinoamericanos, por AP y Alexis Jéldrez, Diario El Mercurio, Cuerpo A10, Martes 29 de Abril 2003.

[54] Protección de la vida privada: EE.UU. COMPRA DATOS DE LATINOAMERICANOS, por AP y Alexis Jéldrez, reportaje diario El Mercurio, Martes 29 de Abril 2003, Cuerpo A.

Por lo tanto, según la opinión de Jijena, no existe un marco jurídico que prohíba este tipo de actos, y cuando se intentó legislar, se inventó esta categoría de fuentes públicas.

B) DOCTRINA ESPAÑOLA

En el art. 18.3 de la Constitución española, se garantiza el secreto de las comunicaciones, dentro de lo cual se incluye la Internet. En relación a ello, la *Agencia de Protección de Datos Española* en sus Recomendaciones a Usuarios de Internet define las Cookies como el "*conjunto de datos que envía un servidor web a cualquier navegador que le vista, 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*"[55].

Es necesario plantearse la interrogante de si nos encontramos frente ante una supuesta violación al derecho a la intimidad, y paralelamente, si se infringe contra el secreto de las comunicaciones.

Analizando en qué consiste el secreto de las comunicaciones, éste no solamente protege el hecho de la comunicación en sí misma, sino que también involucra acontecimientos externos a ella, como la identidad de los comunicantes, por ejemplo. Por tanto, en el caso particular de las *cookies*, lo que en verdad se está regulando es "*con quién establece conexiones un determinado usuario de Internet*"[56]. Sin embargo, es necesario revisar previamente si realmente nos encontramos frente a un caso de *comunicación* de acuerdo a los contemplados en el art. 18.3 de la Constitución española.

¿Qué se entiende por comunicación? Generalmente, consiste en la transmisión de un determinado mensaje, el cual es captado. No obstante, la definición de cookies no cabe dentro de la nomenclatura comunicación, ya que lo que se capta no es un mensaje, sino la visita que realiza un usuario a una determinado sitio web, ya sea para informarse de su contenido o para contratar la adquisición de un producto o servicio. Por lo tanto, el término comunicación presume la transmisión de un mensaje determinado, lo cual no concuerda con el concepto dado de cookies, es decir, la finalidad de averiguar las visitas hechas a través de la Internet a una página determinada.

Para **Roca** y **Torralba**, la información que obtiene el usuario de una página web particular, no puede entenderse como comunicación propiamente tal, ya que "no se dirige directamente a él, como destinatario designado por el titular de la página, sino que es accesible a todos y no tiene, en consecuencia, carácter privado". Más bien, el concepto de cookies y su licitud, es analizable desde el punto de vista del **art. 18.4** de la Constitución española, que establece que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

[55] Definición dada en "Derecho a la Intimidad: El secreto de las comunicaciones e Internet", por Miquel Roca y Elisa Torralba, pág. 195.

[56] "Derecho a la Intimidad: El secreto de las comunicaciones e Internet", por Miquel Roca y Elisa Torralba, 3.2.1 Cookies.

C) DOCTRINA ARGENTINA

En cuanto al uso de programas informáticos que se caracterizan por tener suma relevancia para las compañías de *marketing online*, ya que pueden registrar los hábitos del usuario de Internet, numerosos autores como Stefano Rodota[57], consideran el uso de dichos programas como un atentado a la privacidad, favoreciendo su prohibición, salvo el consentimiento expreso del consumidor.

Sin embargo, también encontramos una postura diferente planteada por la *Federal Trade Comisión*, que se manifiesta a favor del establecimiento de límites a la recolección de datos personales de los consumidores en la Internet, a través de la notificación al usuario de la recolección de sus datos en la página web, ofreciéndole la posibilidad de poder optar por otra página web.

Ricardo Lorenzetti[58] concuerda con la postura de que existe una clara violación de la intimidad y que se debiera prohibir este tipo de prácticas, basando su argumento en el **art. 1071 bis** del Código Civil argentino, el cual establece "*El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación*". Además, se apoya en el **art. 44** del proyecto argentino sobre comercio electrónico, el cual propone que "*los oferentes de bienes y servicios y los prestadores de servicios intermediarios podrán requerir de sus clientes información pertinente a los fines comerciales específicos en cada caso. Sólo podrán ceder a un tercero esta información, en forma total o parcial, si cuentan con el consentimiento expreso y previo de los interesados. Este consentimiento no estará vinculado a la realización de la transacción*".

[57] Rodota, Stefano, "Liberta, Oportunita, Democracia e Informazione", Internet e Privacy: Quali regole?, Tai del Convengo, suplemento I, bolletino 5, Roma, 1999.

[58] Lorenzetti, Ricardo, "La Protección del Consumidor", pág. 243.

CONCLUSIÓN

Los usuarios de Internet actualmente enfrentan una grave amenaza a su privacidad personal. Cookies en la forma de *banner ads* recolectan datos personales de los usuarios de Internet sin su previo conocimiento o consentimiento, y aquellos en posesión de dicha información personal no enfrentan obstáculo legal alguno en relación al tratamiento indebido de ellos. A su vez, la información puede ser vendida o transmitida a terceros con el propósito de crear perfiles personalizados de los usuarios basados en sus hábitos de navegación. Mientras la Internet promete ser uno de los adelantos tecnológicos más significativos y positivos en la historia de la humanidad, existen peligros de equivalente nivel. Debido a la naturaleza tecnológica y comercial de la Internet, la privacidad personal de los consumidores en los Estados Unidos y alrededor del mundo está en grave riesgo. Navegamos en una tempestad, donde el desarrollo de las relaciones online se llevan a cabo con regulaciones legales ambiguas y poco exactas. Cuando los consumidores navegan la Red, su información personal es recolectada, clasificada, analizada y distribuida inmediatamente y a una velocidad asombrosa. El resultado de ello, es un mundo donde los individuos ya no tienen control sobre sus propias identidades.

Frente a tales dificultades, la FTC y el poder legislativo estadounidense sugirieron la implementación de autorregulación respecto de las cookies y la constitución de perfiles. Sin embargo, dicha solución fue inefectiva al momento de solucionar el problema de la privacidad en la red. En relación a esta crisis a nivel de consumidores, es indispensable que el Congreso estadounidense actúe de manera deliberada y decisiva, ya que el sector privado no puede y no va a autorregularse efectivamente en beneficio de los consumidores norteamericanos. Es por ello que el gobierno federal debe exigir a los operadores de sitios web que provean protecciones adecuadas a la privacidad de los usuarios que visitan sus páginas. Al mismo tiempo, tal mandato legislativo debe ser lo suficientemente flexible como para captar las complejidades de la Internet. Por lo tanto, el Congreso de los EE.UU. debiere aprobar una ley que delegase autoridad discrecional a la agencia tutora en el área informática, mandato que asegure que los sitios web procedan conforme a los principios de notificación, opción, acceso y seguridad. Dicha conducta legislativa otorgará a los consumidores una protección efectiva y sustantiva a su privacidad en línea, permitiendo paralelamente, un desarrollo y crecimiento de esta prodigiosa y revolucionaria tecnología denominada Internet. A través de la implementación de dichos principios, los usuarios de Internet estarán mejor informados y tendrán la opción de proteger positivamente su privacidad, pero tal regulación federal no ofrecerá seguridad ante violaciones de sus derechos, si no ofrece una acción legal concreta.

Sin la existencia de leyes estatales o federales concretas que regulen el derecho a la intimidad, los tribunales norteamericanos se están viendo obligados a analizar las demandas y demás pretensiones, mayoría de las cuales no se enmarcan dentro del tipo de la invasión de la privacidad por el uso en sitios web de cookies y la utilización de perfiles. Para proteger la intimidad de los usuarios de Internet y así asegurar la confianza de los consumidores, la Corte Suprema de los EEUU. debe alterar su interpretación de la privacidad constitucional. A su vez, la razonable expectativa de privacidad debe ser reinterpretada, de modo que permita anticipar las amenazas que puedan constituir nuevas tecnologías para los consumidores.

En resumidas cuentas, en los Estados Unidos no existe una legislación vigente que proteja íntegramente la privacidad de los usuarios en todos los sitios web, y el rol fiscalizador de la Comisión resultó limitado para casos excepcionales. Salvo la Ley de Protección a la Privacidad de Menores Online, el resto de los intentos legislativos han resultado infructuosos.

En una sociedad tecnológica como la nuestra, garantizar la privacidad de todos los consumidores resulta ficticio. Sin embargo, el derecho del titular a obtener y confirmar detalladamente qué información ha sido recolectada a su respecto, y el derecho a modificar, eliminar o bloquear datos personales que estén incompletas o inexactos, y donde compañías han sido prohibidas de transmitir o vender datos sin el consentimiento del usuario, es una realidad efectiva a partir del 25 de Octubre de 1998 para los ciudadanos de la Unión Europea.

Este modelo europeo sobre la protección de datos personales, dado el alto nivel de protección que ofrece para la privacidad de los individuos que forman parte de la Unión Europea, "contribuirá para garantizar una mayor fluidez de información en el mercado único, otorgando mayor confianza a los consumidores y minimizando las diferencias legales entre los estados miembros. Además, la Directiva contiene disposiciones especiales que concilian el derecho a la intimidad con la libertad de expresión"[59].

La Directiva establece un marco legal definido y estable tendiente a garantizar la libre circulación de datos personales. La Directiva tiene por objetivo reducir las brechas legales nacionales relacionadas a la protección de datos, de modo de remover los obstáculos que atentan contra la libre circulación de datos personales en la Unión Europea. Como consecuencia de este cuerpo normativo, toda persona cuyos datos son procesados dentro de la Unión Europea, tendrá garantizado una protección igualitaria de sus derechos, particularmente su derecho a la intimidad, independientemente del estado miembro donde sean procesados sus datos.

La Directiva destaca por sobre otras legislaciones extranjeras, en cuanto al modo que previene abusos contra datos personales, y a su vez garantiza que los individuos objeto de la recolección de sus datos, sean notificados respecto a las operaciones de procesamiento. Este estatuto normativo se encuentra dirigido hacia aquellos que recolectan, conservan o transmiten datos personales como parte de sus actividades económicas o administrativas. Particularmente, la Directiva contiene una disposición que solamente autoriza la recolección de datos para fines específicos, explícitos y legítimos, y sólo podrán ser conservados si los datos son relevantes, determinados y se encuentran actualizados.

La Directiva también contempla el *principio de lo justo*, con el objeto de hacer de la recolección de datos lo más transparente posible, otorgándoles a los usuarios la posibilidad de proporcionar o no su información personal. Además, a los consumidores se les conferirá el derecho a informarse acerca de la identidad de la organización encargada del procesamiento de los datos y los fines para los cuales son procesados. En el caso que los datos sean recolectados por terceras partes, la Directiva contempla una excepción, donde no es obligatorio el deber de informar si éste se hace imposible o involucra esfuerzos desproporcionados.

La Directiva también requiere que toda ley nacional concerniente al procesamiento de datos, tenga una base constituida en razón de cinco puntos o cinco temas relevantes, que son: consentimiento, contrato, obligación legal, interés vital del sujeto objeto de la

[59] Cita del Comisionado del Mercado Único, Mario Monti, 25 de Julio de 1995.

recolección, y un equilibrio entre los intereses legítimos de las personas controlando los datos y los individuos objeto de los datos conservados.

Bajo esta Directiva, los individuos afectados por la recolección o procesamiento de datos, poseen una serie de derechos, como el derecho de acceso a los datos, el derecho a saber donde se originó la información, el derecho para que se rectifique los datos inexactos, y el derecho a indemnización en caso de procesamiento ilegal.

Respecto de los datos sensibles, tales como el origen étnico o racial de un individuo, sus creencias religiosas o políticas, su asociación a algún sindicato o datos concernientes a su salud o vida sexual, la Directiva establece que solamente puede ser procesado con el consentimiento expreso del individuo, excepto en casos específicos como en beneficio del interés público; por ejemplo, para investigación médica o científica.

Respecto a la transferencia de datos a países no miembros de la Unión Europea, la Directiva contiene disposiciones que previenen que la normativa europea sea burlada. La regla general establece que aquel país extranjero que reciba datos, debe asegurar un adecuado nivel de protección, aunque también se incluye un sistema práctico de excepciones y condiciones especiales.

La Unión Europea estima la privacidad de datos personales como un derecho fundamental, el cual es protegido de la mejor manera a través de la legislación y la política administrativa. En cambio, los Estados Unidos ha perseguido la protección de datos personales mediante la perspectiva de la autorregulación. Era inevitable que como consecuencia de estas dos ideologías antagonistas, se produjera una confrontación entre la Unión Europea y los EE.UU. en cuanto a la transferencia de datos personales.

El fundamento de esta disputa se encuentra en el artículo 25 de la Directiva de la Unión Europea que entró en vigencia el 25 de Octubre de 1995. Esta disposición prohíbe la transferencia de datos a cualquier país que no cuente con un “adecuado” nivel de protección, según lo determinado por la Unión Europea. Según la opinión de la UE., los Estados Unidos es uno de los países que no cumple con los estándares para la protección de datos personales.

Si los EE.UU. es incapaz de cumplir con los estándares de adecuación de la UE., y la Directiva es aplicada estrictamente, ello se traduciría en severas implicancias para los millones de datos que se transfieren cada día vía la Internet entre los Estados Unidos y Europa. Por ejemplo, una empresa de tarjetas de crédito de los Estados Unidos quizás sea incapaz de realizar un perfil financiero en su base de datos radicado en Los Angeles respecto a un consumidor italiano. Igualmente, una compañía estadounidense enfrentará similares complicaciones al intentar transferir datos de un trabajador europeo a las oficinas centrales radicadas en Nueva York. Similares dificultades surgirán en variados sectores de la industria, donde se realice la recolección y procesamiento de datos. Esto incluye a la prensa, instituciones educacionales, empresas de telecomunicaciones, salud, líneas aéreas, marketing y bancos.

Afortunadamente para estas industrias, la Unión Europea acordó no interrumpir el flujo de datos entre Europa y los Estados Unidos. El Departamento de Comercio de EE.UU. y la Comisión Europea negociaron un acuerdo que permite la continuación de la circulación de datos entre ambas partes. Los Estados Unidos sugirió para las empresas norteamericanas una propuesta voluntaria que se asemeja a los requerimientos exigidos por la Directiva de la Unión Europea, logrando de este modo un “adecuado” nivel para la transferencia de datos. Bajo esta propuesta, un puerto seguro fue creado para que las empresas estadounidenses tengan la opción de adherirse a ciertos principios de privacidad.

Estos denominados principios de puerto seguro involucran exigencias como la notificación, la opción, transferencia directa, seguridad, integridad de los datos, acceso e imposición de las normas. Sin embargo, organismos pro privacidad critican dicha iniciativa, pues argumentan que existe una grave falta de fiscalización en cuanto a la implementación de dichos principios por parte de las compañías norteamericanas.

Solamente si los EEUU. logra establecer un cuerpo normativo federal más coherente, basado en prácticas leales, y tomando como modelo la Directiva de la Unión Europea, como asimismo suscribir un tratado bilateral sobre protección de datos con Europa, podrá generar un clima de confianza para los consumidores de Internet, permitiendo así que el sistema legal siempre esté un paso más adelante que los avances de la tecnología.

En cuanto al caso particular chileno, eventuales abusos a la privacidad a través de la recolección y tratamiento de datos personales en Internet, deben ser determinados y sancionados por el derecho. Un primer intento fue la ley 19.628, considerada por muchos como poco idónea debido a su permisividad, ya que lo que califica como “fuentes accesibles al público”, permite la recopilación y procesamiento de un enorme caudal informativo sin el consentimiento de los afectados.

Esta ley que entró en vigencia el 27 de Octubre de 1999, pretende regular el tratamiento que los organismos públicos y los particulares efectúen de los datos de carácter personal que se encuentren almacenados en registros o bancos de datos, sean de carácter automatizado o no. Sin embargo, este cuerpo normativo contiene dos problemas particulares que atentan contra la intimidad de los datos personales: excepciones que permiten el procesamiento de datos personales sin autorización previa de los titulares, y la no prohibición de la transferencia transfronteriza de datos personales.

Respecto a la ley 19.628, en primer lugar es necesario resaltar el hecho que sus normas son solamente aplicables a las personas naturales. Por ello, en su art. 2, letra (f), define los datos personales como aquellos relativos a cualquier información concerniente a personas naturales identificadas o identificables. Por tanto, el fundamento tras este estatuto legal, es la protección de datos de carácter personal. Sin embargo, dicha protección es relativa, ya que contiene excepciones donde los datos personales pueden ser procesados sin autorización del titular, cuando dichos datos provengan o son recolectados de fuentes accesibles al público.

La propia ley define las fuentes accesibles al público como registros o recopilaciones de datos personales, públicos o privados, de acceso restringido o reservado a los solicitantes.

En cuanto a esta excepción, la ley 19.628 señala taxativamente tres casos en que deben encontrarse los datos: (1) deben ser de carácter económico, financiero, bancario o comercial; (2) deben estar contenidos en listados relativos a categorías de personas que se limiten a indicar antecedentes como su profesión o fecha de nacimiento; (3) o ser necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Respecto a la transferencia internacional de datos, en un principio el legislador intentó adoptar un marco legal similar a la Directiva de la Unión Europea, la cual exige un adecuado nivel de protección en el país receptor o destino, para que proceda la transferencia de datos personales. Por ello, el proyecto original de la Cámara de Diputados, en su art. 23 establecía: “prohíbase a los responsables de bancos de datos personales transmitir datos personales desde países o con destino a países cuya legislación no ofrezca garantías análogas a las previstas en esta ley...”. Sin embargo, la comisión mixta rechazó la

disposición anterior, ya que era de su opinión que la transferencia internacional de datos era materia que debía ser regulada por un tratado internacional.

Por ende, hoy en día, con razón de la ley 19.628, la transferencia internacional de datos se encuentra permitida, siempre que cumpla con las normas generales de este estatuto legal.

Con motivo de estos inconvenientes legales, muchos miran con buenos ojos la moción presentada recientemente en la Cámara de Diputados referida a la "Privacidad de los Datos Recolectados a través de Internet", dando origen al boletín N° 3003-19, donde se consagra el principio de "autodeterminación informativa", es decir, que en toda recolección y tratamiento de datos personales que se realice por medios electrónicos, el recopilador o procesador deberá obtener autorización previa del titular, sin excepción alguna. Otros autores, como Claudio Magliona[60], consideran que también debiere incorporarse ciertos aspectos necesarios para la ley, como la creación de un registro público de bases de datos; la creación de un organismo administrativo regulador del funcionamiento de las bases de datos; ampliar los casos en que el titular pueda oponerse a un procesamiento de sus datos; y la posibilidad de exigir a los responsables de una base de datos la aplicación de medidas de seguridad concretas para evitar filtraciones. Mientras tanto, solamente queda esperar para apreciar el resultado final legal y práctico del prometido estatuto legal que entraría a regular el futuro de los datos recolectados de Internet.

Tras realizar un análisis comparativo de las situaciones legales existentes en Estados Unidos, Europa y Chile, en relación a las cookies y la protección de datos personales, con el objeto de concluir la investigación, nos aventuramos a proponer una serie de medidas prácticas que pueden ser acogidas tanto por los propios usuarios de Internet, como por los gobiernos que buscan regularizar a través del derecho la situación de la intimidad en los datos personales en la Red.

Antes de que cualquier país entre a analizar el problema de la protección de datos personales, debe reconocer tres circunstancias: (1) la iniciativa de autoprotegerse por parte de los consumidores a la larga fracasará, (2) la autorregulación de la industria sin intervención gubernamental ha fracasado y probablemente continuará fracasando, y (3) la regulación gubernamental sin mecanismos predeterminados de control también fracasará. Una vez que un país admita la poca eficiencia de estos tres métodos, podrá empezar a construir una política de privacidad eficiente que equilibre, tanto los intereses de la industria como de los consumidores.

Primeramente, los gobiernos deben educar a los consumidores. Mientras un gobierno promulgue leyes para proteger a sus ciudadanos, ello no se traducirá en que sus ciudadanos dejen de estar alertas. Al igual que una serie de leyes no protegerá a una persona que deja su billetera a plena vista de un ladrón, un conjunto de leyes no resguardará plenamente a los usuarios que revelen demasiada información personal en Internet. Los propios consumidores deben encargarse de configurar sus administradores de cookies y revisar las políticas de privacidad de los sitios web. Muchas páginas web como por ejemplo *TRUSTe* y *Electronic Privacy Information Center*, dan recomendaciones básicas de cómo resguardar la privacidad de consumidores online. Revistas como *PC Magazine*, comentan los distintos programas y servicios vía Internet, relativos a cookies, que pueden bajar los usuarios en forma gratis. Por lo tanto, es indispensable crear conciencia en los usuarios

[60] CHILE: BREVE ANÁLISIS DE LA LEY 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA, por Claudio Paul Magliona Markovicth, Asociado Carey y Cía Ltda.

de Internet acerca de la necesidad de informarse acerca de los métodos para proteger sus datos personales.

En segundo lugar, los consumidores no deben fiarse acerca de la validez de las políticas de privacidad. El usuario de Internet debe convertirse en guardián de su propia intimidad. Las políticas de privacidad pueden cambiar de la noche a la mañana, y dejar a los usuarios vulnerables. Generalmente, estas políticas son confusas, incompletas e inconsistentes. Por ejemplo, *Amazon.com* solía tener una política que permitía a sus clientes "*opt-out*" de compartir sus datos con terceros, es decir, excluirse de compartir sus datos personales con terceras partes. Tiempo después, *Amazon* decidió modificar su política, eliminando esta posibilidad respecto de todos aquellos que no la habían seleccionado anteriormente. Mientras el derecho a modificar sus políticas de privacidad no debe ser despojada de las empresas, sí deberían tener la obligación de informar a sus usuarios vigentes acerca de cualquier modificación al estatuto de privacidad de la compañía, además de concederse un plazo a los consumidores para poder excluirse de la nueva política y removerse de la base de datos de la empresa.

En tercer lugar, cualquier estatuto que se apruebe relativo a la protección de datos personales, debe sujetarse a prácticas de buena fe en la recolección de datos. Sobretodo, los consumidores deben tener acceso a la información personal, para que puedan corroborar que sus datos personales son completos y exactos. Así, como los gobiernos imponen que los productos alimenticios lleven etiquetas con los valores nutricionales, a los sitios web se les debería requerir tener políticas de privacidad que incluyesen prácticas de buena fe en la recolección de datos en defensa de los consumidores. Por lo tanto, si nuevos estatutos legales no incorporan en forma determinada el tema de las políticas privadas, los operadores *online* simplemente los ignorarán como lo han hecho en el pasado. Dichos mandatos legislativos debieren contener normas imperativas, tales como:

1. Publicar la política de privacidad a plena vista de los usuarios en la página principal del sitio web;

2. Hacer que la política de privacidad resalte, a través de un font más grande y un tipo de color distinto, de modo que sobresalga en la página principal;

3. Exigirle a los operadores de la página web que utilicen un vocabulario básico en la política de privacidad;

4. Facilitarles a los usuarios en aprender sus derechos como consumidores: requerirles a los administradores del sitio que vinculen (tener un link) su política de privacidad a la página web de las agencias de protección de datos;

5. Facilitarle a los usuarios el derecho a reclamar si sienten que un sitio ha violado sus derechos de privacidad: requerirles a los operadores de sitios web establecer *links* a la página de reclamo de las agencias de protección de datos.

Una serie de efectos surgirán a partir de estas medidas. Primero, los usuarios podrán acceder directamente a las políticas de privacidad. Segundo, los consumidores que no puedan entender la política de privacidad de un sitio determinado, tendrán la posibilidad de ir al sitio web de la agencia de protección de datos, donde encontrará explicaciones acerca de qué debieren decir la política de privacidad de un sitio. Por último, si un consumidor considera la política de privacidad de un sitio web como vaga e imprecisa, podrá formular un reclamo simplemente a través de un *click*.

BIBLIOGRAFÍA

1) FEDERAL TRADE COMMISSION MATERIALS, por Barbara Anthony, Practising Law Institute, Abril 2001.

2) COPPA, KIDS, COOKIES & CHAT ROOMS: WE'RE FROM THE GOVERNMENT AND WE'RE HERE TO PROTECT YOUR CHILDREN, por Joseph Zavaletta, Mayo del 2001, Santa Clara Computer and High Technology Law Journal.

3) THE LAW OF ONLINE PRIVACY, por Neil Hayes y Baker & McKenzie, Illinois Institute for Continuing Legal Education, Marzo del 2002.

4) PRIVATE EYES ARE WATCHING YOU: CONSUMER ONLINE PRIVACY PROTECTION--LESSONS FROM HOME AND ABROAD, por Lynn Chuang Kramer, Texas International Law Journal, 2002.

5) ARKANSAS SURFERS AND THEIR PRIVACY, OR LACK THEREOF: DOES THE COMMONLAW INVASION OF PRIVACY TORT PROHIBIT E-TAILERS' USE OF "COOKIES"?, por Bryan T. Mckinney y Dwayne Whitten, University of Arkansas at Little Rock Law Review, 2002.

6) INTERNET PRIVACY: WHO MAKES THE RULES, Richard M. Smith, Yale Symposium on Law and Technology, 2001.

7) SUMMARY OF STATE AND FEDERAL PRIVACY-RELATED LAWS, por Cathy Bump,

Jonathan Hart y Peter Cassat, Junio del 2002.

8) A NEW MILLENNIUM DILEMMA: COOKIE TECHNOLOGY, CONSUMERS, AND THE FUTURE OF THE INTERNET, por Courtenay Youngblood, DePaul-LCA Journal of Art and Entertainment Law, 2001.

9) THE FEDERAL GOVERNMENT AS COOKIE INSPECTOR: THE CONSUMER PRIVACYPROTECTION ACT OF 2000, por Ethan Hayward, DePaul-LCA Journal of Art and Entertainment Law, 2001.

10) THE COOKIE MONSTER: FROM SESAME STREET TO YOUR HARD DRIVE, por Jessica J. Thill, South Carolina Law Review, 2001.

11) ECONOMÍA DIGITAL EN CHILE, Editorial Cámara de Comercio de Santiago, Abril 2000.

12) PRIVACY ON THE INTERNET – AN INTEGRATED EU APPROACH TO ON-LINE DATA PROTECTION, Noviembre 2000.

13) INTERNET PRIVACY: DOES THE USE OF "COOKIES" GIVE RISE TO A PRIVATECAUSE OF ACTION FOR INVASION OF PRIVACY IN MINNESOTA, por Gregg M. Fishbein y Susan E. Ellingstad, William Mitchell Law Review, 2001.

14) THE WAY THE "COOKIES" CRUMBLE: INTERNET PRIVACY AND DATA PROTECTION INTHE TWENTY-FIRST CENTURY, por Rachel K. Zimmerman, NYU Journal of Legislation and Public Policy, 2000-2001.

15) A COMMENTARY ON THE STATE OF ONLINE PRIVACY AND THE EFFICACY OF SELF-REGULATION, por Bill Luther, William Mitchell Law Review, 2001.

16) MEMORANDUM RESPECTO A LA LEY 19.628, por Morales, Noguera, Valdivieso & Besa, del 12 de Julio del 2001.

17) PERSONAL PRIVACY IN THE INFORMATION AGE: COMPARISON OF INTERNET DATA PROTECTION REGULATIONS IN THE UNITED STATES AND THE EUROPEAN UNION, por Domingo R. Tan, Loyola of Los Angeles International and Comparative Law Journal, Agosto de 1999.

18) ONLINE PROFILING: A REPORT TO CONGRESS, por la Federal Trade Commission, Junio del 2000.

19) PORNOGRAPHY, PRIVACY, AND DIGITAL SELF HELP, por Tom W. Bell, John Marshall Journal of Computer and Information Law, 2000.

20) E-COMMERCE: RESHAPING THE LANDSCAPE OF CONSUMER PRIVACY, por Michael S. Yang, Maryland Bar Journal, Julio y Agosto del 2000.

21) PROTECTING PRIVACY WITH DECEPTIVE TRADE PRACTICES LEGISLATION, por Jeff Sovern, Fordham Law Review, Marzo del 2001.

22) UPDATE ON INTERNET ADVERTISING AND PROMOTIONS, por Linda A. Goldstein, Practising Law InstitutePatents, Copyrights, Trademarks, and Literary Property Course Handbook Series, Febrero del 2002.

23) INTERNET PRIVACY OR INFORMATION PIRACY: SPINNING LIES ON THE WORLD WIDEWEB, por Michelle Z. Hall, New York Law School Journal of Human Rights, 2002.

24) PRIVACY ON THE INTERNET: STATUTORY AUTHORITY, ENFORCEMENT AND POLICY, por Lori A. Schechter y Sarah H. Phan, Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, Junio del 2002.

25) Protección de la vida privada: EE.UU. COMPRA DATOS DE LATINOAMERICANOS, por AP y Alexis Jéldrez, reportaje diario El Mercurio, Martes 29 de Abril 2003, Cuerpo A.

26) LA PROTECCIÓN DEL CONSUMIDOR, por Ricardo L. Lorenzetti, capítulo sobre Programas de registro del navegante, pág. 243.

27) COUNCIL DEFINITELY ADOPTS DIRECTIVE ON PROTECTION OF PERSONAL DATA, documento de prensa IP/95/822 de la Comisión Europea, publicado el 25 de Julio de 1995.

28) DERECHO A LA INTIMIDAD: EL SECRETO DE LAS COMUNICACIONES E INTERNET, por Miquel Roca Junyent y Elisa Torralba, capítulo 3.2.1 sobre Cookies, págs. 195-198.

29) SURFING THE NET SAFELY AND SMOOTHLY: A NEW STANDARD FOR PROTECTINGPERSONAL INFORMATION FROM HARMFUL AND DISCRIMINATORY WAVES, por Tammy Renée Daub, Washington University Law Quarterly, Otoño 2001.

30) INTERNET PRIVACY: AN OXYMORON, por John D. Penn, American Bankruptcy Institute Journal, Septiembre 2000.

31) TRANSLATING PRIVACY VALUES WITH TECHNOLOGY, por Shawn C. Helms, Boston University Journal of Science and Technology Law, verano 2001.

32) A COMMENTARY ON THE STATE OF ONLINE PRIVACY AND THE EFFICACY OF SELF-REGULATION, por Bill Luther, William Mitchell Law Review, 2001.

33) CHILE: BREVE ANÁLISIS DE LA LEY 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA, por Claudio Paul Magliona Markovicth, Asociado Carey y Cía Ltda.

34) COMENTARIOS SOBRE LOS ASPECTOS RELATIVOS A LOS DATOS PERSONALES DE CARÁCTER ECONÓMICO EN LA LEY Nº 19.628, comentarios de la página de la Cámara de Comercio de Chile (www.camaracomercio.cl/html/quienes/comentarios.htm).