PRIVACIDAD[1] E INTERNET: EL PROBLEMA DEL TRATAMIENTO INVISIBLE Y AUTOMATIZADO DE DATOS PERSONALES

RODOLFO HERRERA BRAVO

1. EL ANONIMATO EN INTERNET COMO DERECHO, UTOPÍA Y BASE DE ESTA PROBLEMÁTICA

"Para gozar íntimamente y para amar se necesita soledad mas para salir airoso se precisa vivir en el mundo". Estas palabras escritas por Stendhal en el siglo XIX, presentan un conflicto en el que permanentemente nos encontramos: el respeto a la privacidad vs. la exposición pública de nuestra vida. Por esa razón, las consideramos válidas para describir, en el siglo XXI, la situación que experimentan los usuarios de servicios de Internet, en particular, cuando buscan información diversa navegando por los contenidos de la *web*.

Si observamos lo que a diario nos presenta la publicidad, los estudios que se han escrito, los medios de comunicación y, principalmente, nuestra propia experiencia encontraremos que la mayoría de los cibernautas sólo desarrollan su actividad en la red de forma realmente libre y espontánea dentro de un marco de individualismo de "soledad", que les permita ir de vínculo en vínculo, de página en página, de contenido en contenido, diseñando un camino virtual personal en Internet, que a su vez, le lleve a conectarse con otros, a vivir en el mundo, siendo así fieles a su propia naturaleza social.

Esa necesaria soledad, usando la expresión de novelista francés, ha llevado a que la doctrina propugne el reconocimiento de un derecho específico emergente para los usuarios de Internet; un derecho al anonimato, en cuya virtud se permita no dejar indicios electrónicos en la comunicación por la red, por ejemplo mediante el uso de seudónimos, procedimientos criptográficos o el empleo de filtros. Además, atendida su estrecha vinculación, se le considera como un elemento esencial en el sistema de protección de datos personales en Internet[2] .

Se trata, entonces de reconocer de forma jurídica que el anonimato en un entorno en línea a diferencia de las comunicaciones en persona (*off-line*), aparece espontáneamente natural al cibernauta que lo pretende en su calidad de tal porque, al menos en un principio, el esfuerzo radica en el establecimiento de la real identidad del usuario de Internet[3] . Así, la anonimia puede ser concebida como una facultad que exige ser respetada para que, consecuencialmente, haga frente a las desigualdades de trato que se dan en ciertos contextos, basadas en criterios raciales, sexuales o de apariencia física. Además, pretende facilitar la participación de personas que en ciertas actividades pueden ser más propensas, a no decir lo que piensan, a menos que el sistema les garantice, la ocultación de sus señas.

En tal sentido, el anonimato de las comunicaciones aparece como un tema relevante, ya que está vinculado no sólo a la vida privada y la protección de datos sino también a otros derechos como la libertad de expresión de los usuarios y el derecho a la inviolabilidad de las comunicaciones privadas. En el primer caso, el anonimato facilita el participar libremente en la red sin temor a ser seguido por las opiniones que se emitan, y en el segundo, permiten mantener la confidencialidad, sin interceptación o vigilancia, a menos que esté autorizada por la ley.

[1] De un tiempo a esta parte habíamos optado por no utilizar la voz "privacidad", por considerarla un anglicismo no reconocido por la Real Academia Española, ni definido por el legislador, atendidas, además las dificultades que observamos al asimilarla a instituciones de derecho romanista como la intimidad (Véase Herrera Bravo, Rodolfo *"La protección de datos personales como una garantía básica de los derechos fundamentales"*. Revista de Derecho Público de la Agrupación de Abogados de la Contraloría General de la República, año 2, N° 5, mayo/agosto, 2001). Sin embargo, la vigésima segunda edición del Diccionario de la Lengua Española -de octubre de 2001-, la ha incorporado expresamente definiéndola como "el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"; esa razón explica su incorporación en este trabajo.

[2] Corripio Gil-Delgado, María de los Reyes. *Regulación Jurídica de los tratamientos de datos personales realizados por el sector privado en Internet.* Premio de la Agencia de Protección de Datos, Madrid, 2000, pp. 20, 183-197.

[3] Johnson Deborah G., *Ética On-line. La ética de las redes informáticas*. Moralia N° 20, 1997, pp. 77-78; 81- 82.

Sin embargo, lograr una navegación anónima por la *web*, no es del todo posible y a ratos parece algo utópico, no sólo por los intentos políticos de intervenir las comunicaciones electrónicas por razones de seguridad y defensa nacional, persecución de delitos, y primacía de interés público[4] , sino porque técnicamente esta red abierta permite investigar el camino seguido por un usuario, debido a los rastros accesibles que va dejando en los nodos[5] , por los que pasa[6] .

Lo anterior ha llevado a que los usuarios de Internet se vuelvan transparentes como el cristal sin proponérselo y sin poder evitarlo por mucha resistencia que ofrezcan, ya que dichas huellas permiten conocer las conexiones que han establecido, los contenidos seleccionados, con quiénes se comunican, a qué hora, por cuánto tiempo, desde dónde, en qué lugar se encuentran físicamente los términos que utilizan, cuáles son sus gustos, sus necesidades, qué escriben, qué compran, qué piensan ... en fin, sin duda, mucho más de lo que se desearía al navegar por la *web*[7] .

A esta traba técnica que afecta al anonimato se suman las razones económicas que van detrás, ya que para hacer efectivo este derecho se requiere como primer paso, que la industria se anime a desarrollar y usar tecnologías y estándares que minimicen la necesidad de procesar datos personales, permitiendo convertir en anónimas las huellas electrónicas[8]. Sin embargo, este cambio en las empresas no se ve muy claro y auspicioso dado el valor que presenta la información nominativa *utilizada por el marketing* relacional o *one to one*, actividad clave para el comercio electrónico, pero en ocasiones realizada, de modo excesivo.

En efecto, esta legítima y necesaria actividad puede llevar a la realización de algunas conductas que consideramos abusivas de la libertad de información y vulneradoras de la vida privada. Por ejemplo, mediante la utilización de los almacenes de datos o *datawarehouse*, y particularmente a través de las técnicas de análisis como la minería de datos o *datamining* se explota una enorme cantidad de datos desordenados obtenidos de fuentes diversas de acceso público del tráfico y la facturación por el uso de dichos servicios de telecomunicaciones de la relación comercial establecida entre las partes de tratamiento invisible u otras, lo que permite descubrir relaciones sutiles u ocultas entre elementos que constituyen la información de las bases de datos y luego generar modelos predictibles derivados de ellos.

Por lo tanto, nos adentramos en una problemática circunscrita al respeto de derechos de los cibernautas que se ven fácilmente desconocidos en el ambiente *on-line,* a causa de la dificultad técnica, política y económica para mantener una situación que permita la navegación libre,

[4] Dicha intervención se ve justificada por estos intereses superiores a los individuales, siempre que guarde proporcionalidad, tenga un carácter excepcional y esté limitada temporalmente, situación que no admite, en cambio en las interceptaciones realizadas por el sector privado, incluso sancionadas penalmente en el artículo 2 de la ley No. 19.223, ("el que con ánimo de apoderarse usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigada con presidio menor en su grado mínimo a medio"), Lamentablemente la intervención estatal se ha visto agudizada por los atentados terroristas sufridos por Estados Unidos quien ha involucrado a importantes países desarrollados, en lo que a nuestro juicio, es una maniquea, contradictoria y violenta campaña contra el terrorismo, que en el plano de las comunicaciones electrónicas se traduce en fuertes restricciones a los derechos individuales de los cibernautas, de la privacidad, y más aún de derechos emergentes como el del anonimato.

[5] Un nodo, es en general, cualquier computador, periférico, o dispositivo como un teléfono celular, conectado directamente a una red.

[6] Cada vez que un cibernauta visita un sitio *web*, se registra un dato en un archivo log del servidor. Ellos tienen programas para transformar esa cantidad de archivos en una información clara, analizando, por ejemplo, el orden por las cuales las páginas *web* han sido visitadas, dando cuenta así de los intereses y decisiones adoptadas durante las visitas.
Esta acción puede no lesionar la privacidad en la medida en que se utilicen los datos, disociadamente, es decir, no pueden asociarse a una persona determinada o determinable. Sin embargo en otras ocasiones lo que realmente interesa es conocer la identificación de quienes acceden, así por ejemplo, para *marketing* directo y ahí es necesario aplicar un sistema de protección de datos nominativos.

[7] La Agencia de Protección de Datos de España, en su memoria de 2000 indica, que sobre la base de su experiencia, las actividades que utilizan Internet como medio de recogida y tratamiento de datos personales son el comercio electrónico, los portales de contenido diversos, los prestadores de telecomunicaciones, la recopilación de direcciones, la gestión de anuncios, las páginas *web*, de temas diversos, las empresas convencionales que han instalado algún tipo de servicio en la red, y la gestión de la moneda virtual. Agrega que los dos tipos de datos de carácter personal que se recogen en las actividades recién mencionadas son datos de mera identificación (nombre, apellidos, dirección de correo electrónico) datos de características personales (fecha de nacimiento, sexo, nacionalidad), datos académicos y profesionales (formación y titulaciones), datos de circunstancias sociales (aficiones y estilo de vida), datos de detalle de empleo (profesión, datos no económicos, de remuneración, historial del trabajador), datos económico-financieros (tarjetas de crédito, datos bancarios), y datos de transacciones (bienes y servicios recibidos por el usuario).

[8] User´s Declaration. European Ministerial Conference, Bonn, 1997. Forum Information Society Report 1997, p.66.

espontánea y personal por la *web*, como podría acontecer si existiera un anonimato efectivo en la red.

En ese contexto, el respeto a los derechos de los cibernautas lo abordaremos en relación con el momento en que un tercero recoge datos de un navegante en Internet, especialmente cuando ello ocurre de modo oculto al usuario, sin su conocimiento ni consentimiento, a través de dispositivos técnicos que operan automáticamente al navegar, operación denominada como tratamientos invisibles.

2. LA RELACIÓN DE LA INFORMACIÓN A LA LUZ DE LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS

El problema del tratamiento de datos en Internet y, en especial, cuando no se realiza de un modo trasparente al usuario radica en la cantidad de información nominativa de éste que otros puedan conocer cuando utiliza servicios de la red. No sólo nos referimos a los datos que directamente conciernen a una persona natural identificada, como su nombre o su dirección, sino también a aquellos que pueden vincularse indirectamente a un individuo mediante un simple cruce de datos con los archivos de clientes de los proveedores de acceso, por ejemplo.

En efecto, no hay que olvidar que al comenzar una sesión en Internet[9], el ISP (Proveedor de Servicios de Internet) asigna a cada usuario un número único (conocido como IP dinámico) y anota los tiempos de conexión en unión con este número, formando una base de datos. En otro listado almacena la identificación de los usuarios y su número. Esta dirección IP dinámica aparece en todas las páginas que se visitan en la *web*, permitiendo deducir el proveedor y el país del cibernauta, e incluso analizando los *logs* es posible localizar desde que número de teléfono llamó, el día y hora, o qué terminal es. Por lo tanto, cuando se cruza la base que contiene los datos de conexión con los números IP se les vincula con los usuarios, se revelan datos de carácter personal.

En tales circunstancias, la protección de la privacidad en Internet, necesita fortalecerse principalmente al momento de la recolección de datos, sean estos recabados del propio titular, de fuentes accesibles al público o del procesamiento de "información persistente del cliente", es decir, de datos relacionados con el computador del usuario y que permanecen más de una sesión en el equipo informático denominado "cliente". La razón de este refuerzo estriba en que una vez reunidos los datos personales de los cibernautas, aquellos quedan fuera del control de su titular y, por aplicación del principio de territorialidad de la ley, si circulan transfronterizamente como suele ocurrir en Internet, el marco jurídico del país de origen podría no tener fuerza totalmente vinculante. No obstante, este último es un tema que, pese a su importancia e interés, no desarrollaremos en este trabajo porque escapa del objeto central de nuestra investigación.

Nos parece relevante propender hacia una recogida respetuosa de los principios básicos reconocidos en los sistemas de protección de datos personales. Al respecto la ley N° 19.628, sobre la protección de la vida privada, pese a todas sus imperfecciones[10], reconoce que el tratamiento sólo puede efectuarse cuando el titular consienta expresamente en ello (artículo 4 inciso primero); se le informa debidamente del propósito del almacenamiento de sus datos y su posible comunicación al público,(artículo 4 inciso segundo); se utilizan los datos sólo

[9] Una sesión comienza cuando se solicita una página en un sitio *web* determinado y termina cuando el usuario decide cerrar el programa de navegación apagando el computador o solicitar una página de otro sitio *web*.

[10] Sin profundizar en esta oportunidad en nuestra crítica a la regulación establecida por la ley N° 19.628, sobre Protección de la Vida Privada mencionaremos algunas. Primero, nos parece que la protección de la vida privada que orientó desde sus orígenes las discusiones parlamentarias y a la que alude incluso la denominación de la Ley, cede a veces en exceso, ante los derechos del responsable del registro a causa de la insuficiencia de algunas garantías. Segundo, contiene demasiadas disposiciones especiales para ciertos datos contenidos en fuentes accesibles al público que quita terreno a los normas de protección ordinaria. Tercero, en los sistemas de protección de datos el titular cuenta con un derecho para acceder a cierta información relevante que le concierne, piedra angular a partir de la cual es posible ejercitar otras facultades, como la rectificación, la cancelación o el bloqueo de los datos. Sin embargo, para hacer efectivo este derecho de acceso y, consecuencialmente, los otros, se garantiza que el titular pueda saber quién está utilizando sus datos, para qué fines se están tratando, y si están siendo comunicados a terceros, gracias a que, previo al tratamiento es necesario notificar este hecho a un órgano de control independiente, que mantiene un registro al efecto y cumple un rol, fiscalizador y sancionador, entre cuya creación se omitió bajo débiles argumentos. Además debería contemplar un derecho al recurso -por vía administrativa, civil o, incluso, penal-, con sanciones y responsabilidades para quienes incumplan las disposiciones legales.
Nos parece que el legislador sólo entendió un parte de este entramado, ya que se limitó a reconocer tales facultades, pero luego, las dejó carentes de eficiencia práctica al no crear un órgano especializado encargado de velar por el cumplimiento de la Ley. Lo anterior, unido a otras omisiones graves, por ejemplo, en materia de seguridad en la necesidad de consentimiento del titular para realizar las comunicaciones a terceros o en relación con la transferencia internacional de datos lejos de tratarse de críticas meramente formales o de segundo orden, son errores esenciales del legislador que reafirman nuestra opinión sobre la Ley N° 19.628, y nos llevan a concluir que en Chile aún está pendiente el tema de la protección de datos personales.

para los fines para los cuales hubieren sido recolectados (artículo 9 inciso primero); y siempre que la información sea exacta, actualizada y responda con veracidad a la situación real del titular de los datos (artículo 9 inciso segundo). En definitiva, las disposiciones contienen un deber de información y los principios que la doctrina denomina como calidad de los datos, consentimiento del titular y finalidad del tratamiento.

Dichos principios, vinculados con un tratamiento leal y legítimo, se encuentran reconocidos en el convenio 108, de 1981, suscrito en Estrasburgo por el Consejo de Europa, relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, uno de los primeros pilares jurídico-positivos de carácter internacional sobre la materia. En su artículo 5 dispone que los datos de carácter personal sean objeto de un tratamiento automatizado, se obtendrán y tratarán leal y legítimamente y no se utilizarán de una forma incompatible con éstas; serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado, serán exactos y si fuere necesario puestos al día, y se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Catorce años después la misma norma se repite, ahora en la Directiva[11] 95/46/CE del Parlamento Europeo y del Consejo, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en cuyo artículo 6.1 establece lo siguiente:

> *Art. 6.1: Los Estados miembros dispondrán que los datos personales sean:*
>
> *a) tratados de manera leal y lícita*
> *b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; [...]*
> *c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.*
> *d) exactos y, cuando sea necesario, actualizados; [...]*
> *e) conservados en una forma que permitan la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriomente [...].*

Además, la directiva agrega en el artículo 7 como principio relativo a la legitimación del tratamiento de datos que el interesado haya dado su consentimiento de forma inequívoca.

Finalmente, nos parece interesante mencionar como demostración de un criterio que ha permanecido por los años lo dispuesto en la Carta de Derechos Fundamentales de la Unión Europea, la cual , en diciembre de 2000 estableció en su artículo 8 que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan; que estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley[12] .

De conformidad con lo anterior, una recogida leal de datos en Internet supone que quien los colecte despliegue toda la diligencia necesaria para cumplir las condiciones de licitud, los obtenga de forma totalmente transparente y prevenga los riesgos que ese acto puede conllevar para el titular de los datos. En particular, la lealtad debe venir referida a los medios utilizados para la recogida, a la entrega de información previa al interesado y a contar con su consentimiento libre, inequívoco, específico e informado[13] .

La lealtad también se manifiesta al limitar la recogida sólo a aquellos datos necesarios para alcanzar las finalidades propuestas y, al cancelarlos una vez cumplidos dichos fines. Por eso, una colecta leal exige la definición lo más precisa posible de la finalidad que se persigue, no siendo correcta una descripción vaga del objeto del tratamiento, como por ejemplo al señalar “fines comerciales”.

Por otra parte cabe destacar la directa conexión que presenta el deber de información al titular con el principio del consentimiento, sea

[11] La Directiva es un tipo de norma comunitaria que obliga al Estado miembro destinatario, en cuanto al resultado a obtener, dejando a éste la elección de la forma y medios a emplear . Su objetivo principal es la aproximación entre las legislaciones de los distintos Estados de la Unión. En virtud de las mismas los Estados miembros deben adecuar su legislación a las normas comunitarias, suprimiendo, modificando o generando normas adecuadas. Lo vinculante es el objetivo comunitario a alcanzar, no la forma y medios. Una directiva puede ser de efectos directos para los ciudadanos del Estado. UII. Pont. Eugenio. *Derecho Público de la Informática (protección de datos de carácter personal).* UNED Ediciones, Madrid. 2000. pp. 295-296.

[12] Hemos limitado nuestra revisión de ordenamientos extranjeros solamente a estos cuerpos normativos europeos, sin referirnos a ordenamientos anglosajones, asiáticos o latinoamericanos, por considerar que en los que mencionamos se han abordado seriamente el tema y por gozar de la generalidad y amplitud necesaria para comenzar a conocer los sistemas de protección de datos en países como Chile, en donde, a nuestro juicio, hoy es un tema desconocido o, al menos insuficiente e imperfectamente desarrollado.

[13] Hemos destacado estas características del consentimiento basados en la definición que de él realiza la ley española 15/1999, sobre la protección de datos de carácter personal, en su artículo 3 letra h.

que los datos se recaben de él mismo o no. En la Unión Europea se sigue el criterio contenido en el artículo 10 de la Directiva 95/46/CE antes mencionada, según el cual se debe explicitar a lo menos la identidad del responsable del tratamiento[14], los fines a que van a ser objeto los datos, sus destinatarios o categorías de éstos, el carácter obligatorio o no de la respuesta del titular, las consecuencias que tendría para él, su negativa a responder, la existencia de derechos de acceso y rectificación que pueda ejercer y, habida consideración de las circunstancias específicas en que se obtienen los datos, toda información suplementaria necesaria para garantizar un tratamiento leal.

En Chile la ley N° 19.628, en los artículos 4 y 5 ha dispuesto que la utilización escrita del titular al tratamiento de sus datos debe haber estado debidamente informada respecto al propósito del almacenamiento y su posible comunicación. En este último caso frente a requerimientos de datos personales que un tercero haga mediante una red electrónica se debe dejar constancia de la individualización del requirente; el motivo y el propósito del requerimiento, y el tipo de datos que se transmiten. En este supuesto, el receptor sólo puede utilizar los datos personales para fines que motivaron la transmisión.

Cabe advertir que aunque la misma ley establece que la necesidad de consentimiento y el deber de información no son aplicables cuando se trata de datos personales accesibles al público en general, es decir, cuando provengan de registros o de recopilaciones de datos nominativos, públicos y privados de acceso no restringido o reservados a los solicitantes, ello no significa necesariamente que esa información no tenga un titular o que éste renuncie a sus derechos.

En virtud de lo anterior, una situación en la que se podría considerar leal la recogida de datos desde el punto de vista del deber de información se presentaría cuando la página *web* en donde se solicitan datos personales indica la política de privacidad de la empresa, señalando su identificación precisa; un correo electrónico y una dirección postal para el ejercicio de los derechos de acceso, ratificación, cancelación y para especificar las finalidades para las que se autoriza el uso de los datos; el que la captación de información sea almacenada en el equipo informático y el tipo de datos que recoge; la finalidad o finalidades a que se destina la información obtenida; y la atención de comunicar los datos a terceros.

3. ¿CUÁNDO HAY UN TRATAMIENTO INVISIBLE DE DATOS PERSONALES?

Como hemos visto, navegar por Internet deja tras de sí un sinnúmero de datos que quedan registrados en los nodos por los que pasa un cibernauta cada vez que ingresa a una página *web*, por lo que es necesario garantizar un tratamiento leal, principalmente al momento de la recogida de éstos, mediante el respeto de un conjunto de principios básicos de los sistemas de protección de datos de carácter personal.

Sin embargo, en Internet no siempre se reúnen datos con consentimiento del titular; incluso hay ocasiones en las que ni siquiera se cuenta con su conocimiento, privándole la posibilidad de ejercitar sus derechos.

Precisamente en este caso se presenta el denominado "tratamiento invisible y automatizado de datos personales", que consiste en un conjunto de operaciones y procedimientos técnicos efectuados por programas y equipos capaces de procesar los datos de los usuarios y ponerlos a disposición de terceros sin conocimiento o consentimiento de sus titulares.

Ahora bien, ¿cuándo se realiza este procedimiento tan particular? Sus manifestaciones son múltiples, algunas más conocidas que otras. Lo encontramos en los hipervínculos o enlaces automáticos a sitios de terceros que incluyen en las páginas web, o cuando el servidor envía contenido activo, como Javascript[15] o ActiveX [16].

[14] El legislador chileno emplea la denominación responsable del registro o banco de datos, para referirse al responsable del tratamiento.

[15] *Javascript* es un lenguaje de programación desarrollado por *Netscape* para hacer más conveniente la animación y otras formas de interacción. Estos programas se encuentran en archivos HTML y les permiten a éstos controlar el *browser* o navegador. En cuanto a los ataques a la privacidad cabe advertir que, como el código de *JavaScript* descargando corre dentro del navegador, potencialmente tiene acceso a cualquier información que este tenga. Por lo tanto el problema de JavaScript pasa más que por el tener acceso a información sensible, por el que ésta pueda salir del computador del usuario. Véase Garfinkel, Simson y Spafford, Gene. *Seguridad y comercio en el web.* Ed. Mc Graw-Hill, México , 1999.

[16] Actives es un conjunto de tecnologías, protocolos e interfaces de programación desarrollados por Microsoft, que sirven para descargar códigos ejecutables de Internet. Como riesgo destaca la posibilidad de apoderarse de información privada y confidencial. Véase Garfinkel, Simson y Spafford, Gene.*Op. Cit.*

También puede haber un tratamiento invisible a partir de la actuación que realiza un "agente inteligente", es decir, un programa informático configurado por una persona para cumplir una misión y tomar una decisión. En estas aplicaciones se observa una triple función: filtrar información en función de los parámetros fijados; personalizar el interfaz adoptándolo automáticamente a las necesidades del usuario; y recogiendo información autónomamente porque estos agentes son capaces de actuar incluso aunque el usuario no esté conectado a la red, todo lo cual implica que no exista un control o supervisión directa del usuario para el que actúa[17].

Los programas navegadores o *browsers* -como *Internet Explorer, Navigator* u *Opera* por ejemplo- constituyen otro caso en el que se realiza tratamiento invisible. Estos programas destinados entre otras cosas a visualizar gráficamente el material disponible en Internet y a comunicar el cliente (computador del usuario) con el servidor *web* (computador remoto donde está almacenada la información), envían automáticamente a éste más información de la estrictamente necesaria para establecer la comunicación, por ejemplo el tipo y la lengua del navegador, el nombre de otros programas instalados en el computador y el sistema operativo del usuario, entre otros. A estos se suman la posibilidad de que el navegador, también de manera invisible transmita sistemáticamente esos datos a terceros.

Por otra parte, la manifestación de tratamiento invisible más conocida es, sin duda, la conformada por archivos denominados *cookies*, que se envían desde un servidor al computador de un usuario con el objeto de identificar en el futuro ese equipo en sucesivas visitas al mismo sitio *web*.

La función básica de un *cookie* es permitir a un servidor almacenar y más adelante, recuperar una pequeña cantidad de información en la máquina cliente, guardando aquellos *datos* que expresamente determine un archivo de texto. Esos datos que contiene -dentro de los que podría incluir alguna información personal, cómo códigos de usuario y contraseñas- están asociados a un sitio *web* y a un programa navegador en particular, lo cual implica que un *cookie* creado por un servidor en un momento dado sólo será accesible en el futuro si el visitante regresa al sitio *web* usando el mismo computador y el mismo navegador[18].

Sin embargo, no todos los *cookies* son iguales, los hay locales y remotos. Los *cookies* locales son los que señalamos procedentes y pueden ser tan necesarios que algunos sitios dependan de ellos para trabajar correctamente, por ejemplo, para acceder a cuentas de correo *webmail* como *Yahoo* o *Hotmail* o para comprar libros o música en sitios como *Amazon*. En cambio, los *cookies* remotos son los que hacen posible el funcionamiento de redes de seguimiento de la navegación que realiza un usuario. Suelen guardarse cuando el sitio *web* que se visita despliega publicidad de terceros a través de *banners* o *applets* Java, es decir mensajes comerciales que poseen la capacidad de ejecutar un código que puede grabar el *cookie* en un cliente, y recuperarlo posteriormente. Así, analizando los datos que va dejando registrado el usuario en los *cookies* remotos técnicamente es posible vigilar las acciones de los usuarios en la red.

Por tanto, lo anterior nos lleva a concluir que frente a la existencia de técnicas que permiten crear registros a partir de los vínculos por los que ha pasado el usuario y que están almacenados en el servidor -que contienen información sobre el comportamiento, la identidad, el recorrido efectuado o las elecciones expresadas por la persona al visitar el sitio web-, quienes navegan por Internet deben morigerar el resguardo celoso de su vida privada y volverse tolerantes, permitiendo que otros traten dicha información. Sin embargo, la justa medida de ello se encuentra en un equilibrio suficiente que permita que esa tolerancia del individuo para con el medio pueda transformarse legítima y eficazmente en firme oposición allí donde el exceso y el abuso dañen su dignidad y conculquen sus derechos.

4. PRESUPUESTOS RECOMENDADOS PARA UN TRATAMIENTO INVISIBLE DE DATOS NOMINATIVOS LEAL Y LICÍTO

Como los cibernautas no son conscientes de que constantemente

[17] En el comercio electrónico los agentes inteligentes tienen aplicaciones particulares destinadas a buscar la oferta de un producto, comparar precios y ofrecer información clasificada por las preferencias del usuario.

[18] Es frecuente almacenar la fecha de la última visita, o bien algunos datos que permitan "recordar" lo que el usuario hizo o adquirió en esa oportunidad. Así, en el momento en que la persona regresa al sitio, su navegador envía el contenido del *cookie* al servidor , para que lo interprete y use de un modo preestablecido, por ejemplo, mostrando un saludo personalizado al usuario.

se está recopilando información que les concierne y desconocen los fines a que se destinan sus datos, el tratamiento invisible que no se realiza de forma totalmente transparente al usuario contraviene el principio de lealtad en la recogida de datos e impide el ejercicio de los derechos que le asisten, especialmente, el de acceso, incluso, pese a saber la existencia de dicho tratamiento, no está en condiciones de entender el significado de las informaciones grabadas en el *cookie*, por ejemplo. Por esa razón, finalizaremos este trabajo planteando algunas recomendaciones para que el tratamiento invisible sea formado, consentido y, en definitiva lícito y leal.

Según hemos señalado precedentemente, la legitimidad de estas operaciones y procedimientos técnicos descansa sobre dos pilares básicos; información y consentimiento. El primero de ellos consiste en el deber de suministrar información suficiente sobre los datos que se pretenden recopilar, almacenar o transmitir, la finalidad del tratamiento y los derechos a oponerse al registro de ciertas categorías de servicios consultados cuando sean capaces de mostrar, además del perfil del consumidor potencial, sus hábitos, tendencia sexual, opiniones políticas o religiosas, es decir, datos sensibles. Recordemos que ese tipo de información cuenta con una protección reforzada en la ley N°.19.628 antes anotada, la cual prohíbe su tratamiento a menos que una ley autorice, sean datos necesarios para determinar u otorgar beneficios de salud a sus titulares, o cuenten con el consentimiento escrito del titular.

Además, una información de buena fe no debe limitarse sólo a indicar que se generará un *cookie* o que los datos serán conservados con fines de promoción comercial, sino que será preciso que el usuario tenga noticia clara de la identidad del responsable del tratamiento de los fines perseguidos, las categorías de datos, los destinatarios de éstos, y la existencia de derechos de acceso y rectificación.

Lo anterior, llevado a la práctica, significa que los *browsers* deberían señalar al momento de establecer una conexión con el servidor *web*, qué datos se pretenden transferir y con qué objetivo. Tratándose de *cookies* el usuario tendría que ser advertido cuando esté previsto que el *software* de Internet, los reciba, almacene o envíe, especificando en un lenguaje comprensible qué información se pretende guardar en el *cookie,* su finalidad y el periodo de validez[19].

Como consecuencia de ello, estos dispositivos no deberán estar configurados para que por defecto se recopile, almacene o remita "información persistente del cliente", que como explicamos es la que permanece más de una sesión en el equipo informático del usuario. En tal sentido, la opción por defecto del navegador sólo debiera permitir el tratamiento de la mínima cantidad de información necesaria para establecer una conexión y, en el caso de los *cookies* no deberían ser enviados ni almacenados de forma oculta[20].

El segundo pilar es, obviamente, el consentimiento expreso y facilitado desde los propios programas de navegación. Los productos de Internet, tanto de *software* como de *hardware* deberían permitir al interesado decidir libremente sobre el tratamiento de sus datos personales ofreciéndoles instrumentos de fácil manejo para filtrar la recepción, el almacenamiento o el envío de la información persistente del cliente según unos criterios determinados, tales como perfiles, dominios o identidad del servidor, o el tipo y duración de la información, recopilada, almacenada o enviada.

En este sentido, un *browser* debería brindar la opción para que el usuario lo configure especificando el tipo de información que debe o no recopilar y transmitir. En el caso de los *cookies*, el usuario debería contar siempre con la opción de aceptar o rechazar su envío o almacenamiento, junto con disponer de alternativas para determinar los elementos de información que se van a conservar o eliminar de un *cookie,* considerando, por ejemplo, el período de validez o los sitios *web* de envío y recepción.

Además, se recomienda establecer en los programas la posibilidad de eliminar la información persistente del cliente de manera simple para el usuario e inocua para el remitente. Incluso cuando no sea posible eliminar dicha información tendría que existir una forma fiable para evitar su transferencia y lectura, todo lo cual se logra en la medida que los *cookies* y demás información persistente del cliente

[19] Véase la recomendación 1/99 de 23 de febrero de 1999, sobre el tratamiento invisible y automático de datos personales en Internet adoptada por el Grupo de trabajo del artículo 29 (Grupo europeo especializado en protección de datos personales, creado por el artículo 29 de la Directiva 95/46/CE).

[20] Recientemente el Consejo de Ministros de Telecomunicaciones de la Unión Europea ha alcanzado un acuerdo sobre la Directiva referente a la privacidad a las comunicaciones electrónicas norma que compromete ha organismos públicos y privados a destruir y hacer anónimos los datos personales que obtengan a través sus comunicaciones en Internet, excepto si consideran que éstos afectan la seguridad pública o del Estado. En relación con los cookies, a propuesta de Francia, la Directiva obliga a que no puedan activarse sin que el usuario lo haya autorizado al menos en una ocasión.

se almacenen de forma normalizada que permita borrarla selectivamente en el cliente.

En definitiva, frente a un tratamiento invisible y automático necesario para mejorar los servicios ofrecidos por la red, personalizándola o volviéndola más interactiva, la lealtad que lo legitima debe cumplir con prácticas generalmente aceptadas que consisten en la entrega de información clara y completa sobre el procesamiento de datos nominativos que se recopilan, en el ofrecimiento de opciones para los cibernautas relacionados con el tratamiento de su información personal, la facilidad para que el titular acceda de forma razonable a ésta, incluyendo la posibilidad de revisarla, corregir inexactitudes o borrarla; y con la opción de medidas pertinentes para preservar la seguridad de los datos que recolectan de los usuarios.

Son exigencias mínimas para lograr que los usuarios de Internet confíen en el comercio electrónico, para que la tecnología no avasalle los derechos de las personas y para que no se opte, tampoco, por prohibir este tipo de recogida de información ya que ello podría afectar el interés comercial en la red. Sin embargo,... ¿existirá la voluntad suficiente para corregir el estado actual de las cosas? Es una interrogante que debe ser resuelta en parte por los propios usuarios, los principales defensores de sus derechos.

5. BIBLIOGRAFÍA

Agencia de Protección de Datos de España, *Memoria* 1999.

Agencia de Protección de Datos de España, *Memoria* 2000.

Corripio Gil-Delgado, María de los Reyes. *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*. Premio de la Agencia de Protección de Datos, Madrid, 2000.

Garfinkel Simson y Spafford, Gene, *Seguridad y comercio en el web,* Ed. Mc Graw-Hill, 1999.

Herrera Bravo, Rodolfo *"La protección de datos personales como una garantía básica de los derechos fundamentales"*.Revista de Derecho Público de la Agrupación de Abogados de la Contraloría General de la República, Año 2, N° 5, mayo / agosto 2001.

Johnson, Deborah G., Ética On-line. *La ética en las redes informáticas,* Moralia N°20, 1997. Real Academia Española, *Dirección de la Lengua Española*, 22ª edición 2001.

Ull Pont, Eugenio. *Derecho Público de la Informática (Protección de datos de carácter personal)* UNED Ediciones, Madrid, 2000.

USER´S DECLARATION. *European Ministerial Conference,* Bonn,1997, Forum Information Society Report 1997.