INTRODUCCION

La sociedad de la información exige que las empresas tengan implementadas eficaces políticas de protección y seguridad de datos personales. En la medida en que la red informática se ha convertido en una herramienta importante para el comercio electrónico, el interés de las empresas por conocer y tratar datos personales ha aumentando considerablemente; por lo que es necesario una confianza y seguridad suficientes para los sujetos intervinientes.

En consecuencia, los particulares riesgos del tratamiento y la transmisión de los datos personales en el espacio cibernético exponen a los consumidores a prácticas comerciales excesivas, así como a los diversos supuestos de deslealtad o ilicitud en el almacenamiento de los datos, como la generación automática e inconsentida de cookies, registro de hábitos de navegación, la combinación del catering del navegador, los hipervínculos invisibles, los webbugs, los programas espías. Las informaciones recogidas sirven de base para la elaboración de perfiles de los usuarios que visitan las páginas electrónicas comerciales en función de los cuales disponen la publicidad y las ofertas en sus respectivas páginas, o la creación de anuarios de direcciones de correo que se emplean en marketing directo, entre otras acciones.

Este tema es de suma importancia, bajo la hipótesis que la protección de datos personales es un área que requiere de una adecuada salvaguarda en el desarrollo tanto de actividades publicitarias como de transacciones contractuales con los usuarios, realizadas en la Internet. Además es necesario conocer los riesgos a los que se encuentran expuestos los datos de aquellos consumidores que intervienen en el

comercio electrónico, los cuales, en su gran mayoría son desconocidos por los mismos usuarios.

La necesaria protección jurídica de los datos, objeto de nuestro análisis, es un paso a añadir en el elenco legislativo nacional e internacional que regula el comercio electrónico en la sociedad de la información, el cual implica diversas facetas de derechos como la equidad en las prácticas comerciales, las ofertas y las condiciones contractuales, la protección de los datos personales de los menores, la seguridad de los sistemas de pago incluida la firma electrónica, etc.

El propósito de la presente tesis de investigación descansa en demostrar la importancia que en la actualidad tienen las leyes de protección de datos personales para generar confianza en los consumidores que intervienen en el mercado del comercio electrónico. En ese orden de ideas, en el primer Capítulo de este trabajo, describiré las divergencias que existen actualmente entre la necesaria protección de los datos personales y el negocio electrónico. También se expone el distinto trato normativo que diversas legislaciones le han dado a la cuestión en estudio; y el derecho aplicable. No es el propósito de esta investigación referirse a la legislación particular de un país específico, sino exponer los diversos supuestos y aportes de una manera genérica.

Diversos organismos internacionales, como la Organización para la Cooperación y el Desarrollo Económico (OCDE) y la Organización de las Naciones Unidas (ONU); y más recientemente en la Unión Europea, han planteado desde hace algunos años

iniciativas para intentar brindar una solución frente a la problemática de la protección jurídica de los datos de carácter personal en el marco del comercio electrónico.

Luego, en el segundo apartado, se estudia el comportamiento de las partes involucradas y sus obligaciones; el almacenamiento de las base de datos personales en el comercio electrónico. Posteriormente se aborda el análisis de las galletas informáticas "cookies", los correos electrónicos no solicitados y el movimiento transfronterizo de datos personales. Finalmente, en la sección cuarta, se explican las estrategias y/o soluciones que se proponen en la materia.

Luego, en el segundo apartado, se estudia el comportamiento de las partes involucradas y sus obligaciones; el almacenamiento de las base de datos personales en el comercio electrónico. Enseguida, abordaremos el análisis de las galletas informáticas, los correos no solicitados y el movimiento transfronterizo de datos personales. En la cuarta sección, explicaremos las estrategias y/o soluciones existentes en la materia.

El método utilizado para la realización de esta obra fue la investigación a través de fuentes documentales y electrónicas. Es preciso destacar que este tema se encuentra en constante evolución. Este trabajo fue finalizado a inicios del mes de diciembre del 2009 y no refleja las actualizaciones en la materia después de esa fecha. Los vínculos de Internet estaban vigentes en esa fecha.

1.1 Internet y comercio.

Internet revolucionó las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas, lo cual introduce nuevas posibilidades para sus usuarios así como también nuevos riesgos para sus datos personales y su intimidad. Esto se debe a la proliferación de oportunidades que existe en la red, de datos personales y por tanto, el riesgo de incumplimiento de los derechos y libertades fundamentales de las personas, en especial el derecho a la privacidad.

Los servicios que conforman la sociedad de la información son aquellos prestados normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, como por ejemplo, el comercio electrónico. También se encuentran los no remunerados por sus destinatarios en la medida en que constituyen una actividad económica para el prestador de servicios. El comercio electrónico se ha convertido en el nuevo modelo de negocios[1]; es un fenómeno ligado al proceso de

[1] Este puede implicar un amplio rango de operaciones y transacciones comerciales, como las siguientes: a) establecimiento del contacto inicial, por ejemplo, entre un cliente potencial y un proveedor potencial; b) suministro e intercambio de información, bienes y servicios, operaciones financieras, bursátiles y de seguros, consultoría, servicios públicos; c) soporte pre-venta (detalle de los productos y servicios disponibles, cuadros comparativos de precio y características, elementos complementarios, empresas proveedoras de productos adicionales); d) soporte de pos-venta (guía técnica del uso del producto, respuestas a preguntas frecuentes, guía de implementación); e) ventas, subastas, centros comerciales virtuales; f) publicidad; g) marketing (incluyendo sondeos, estudios de mercados, encuestas, etc.); g) pago electrónico (usando transferencia electrónica de fondos, tarjeta de crédito, monederos electrónicos); i) distribución, incluyendo tanto la administración como la logística.

producción y distribución empresarial de bienes y servicios, en el cual participa el empresario.

Se considera comercio electrónico a toda transacción comercial realizada por un medio electrónico, sea o no contractual, estructurada a partir de la utilización de las nuevas tecnologías. En sus comienzos, a los fines del comercio, la red era considerada como un medio a través del cual los empresarios, en círculos cerrados y utilizando redes privadas y propias se transmitían los datos (business to business) y no estaba dirigido a particulares (business to consumers). Con el transcurso de los años y la penetración que Internet ha tenido en la sociedad, esta situación ha cambiado por lo que en la actualidad los destinatarios de la información, publicidad y ofertas son tanto las empresas como los consumidores.

Son innegables las enormes oportunidades y/o posibilidades que el comercio electrónico ofrece a los consumidores y a las empresas. Entre éstas, cabe destacar el bajo costo de negociación entre regiones; las mayores alternativas de elección para los consumidores; la mayor promoción e inversión de bienes y servicios: la creación de nuevos sistemas de obtención de ingresos; la generación de nuevos puestos de trabajo; la eliminación de los gastos de intermediación y la disminución en los costos de publicidad.

1.2 Comercio electrónico vs. Protección de datos personales.

Antes de iniciar el desarrollo de las incidencias del comercio electrónico en la protección de los datos personales de los usuarios de Internet que intervienen en este mercado se torna imperioso definir qué debe entenderse como "tratamiento de datos personales". El tratamiento de datos personales comprende las operaciones y procedimientos sistemáticos, electrónicos o no, efectuadas sobre éstos, que permitan la recolección, conservación, organización, almacenamiento, modificación, relación, análisis, evaluación, bloqueo, destrucción y en general, su procesamiento, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones, transmisiones o transferencias.

Gracias a la tecnología, la interconexión de bases de datos permite la recopilación masiva, instantánea e indiscriminada de datos personales desde cualquier parte del mundo, y transferirlos a terceros u otros ficheros, no importa donde se encuentren. En efecto, las bases de datos pueden actuar como una central de registro universal de la información personal o como parte de una red global de la cual se alimenta la central. Todo lo que un usuario ha suministrado a las diferentes bases de datos de diversas partes del mundo puede ser unido o compilado. De ahí resulta que en cualquier momento cabe la posibilidad de tener acceso a los datos personales de un tercero, los cuales podrían ser utilizadas para fines distintos y desconocidos por su titular.

En la medida en que el desarrollo de Internet y las autopistas de la información se han convertido en herramientas para el comercio electrónico, el interés de las empresas por conocer y tratar datos personales de sus clientes actuales o potenciales ha

aumentado considerablemente. Cuanta más información obtengan, será mejor ya que su supervivencia y éxito empresarial pueden depender de la cantidad y profundidad de ésta. Requieren estas informaciones, especialmente, para las áreas de servicios de telecomunicaciones, servicios financieros, marketing directo y laboral. La acumulación es exponencial, automatizada y realizada por defecto en cualquier operación del comercio electrónico.

Igualmente nuestros datos personales se han convertido en un factor esencial para la toma de decisiones de los sectores público y privado de cualquier sociedad. La importancia de tal información, sumada a su fácil y expedito tratamiento gracias a la tecnología, han convertido los datos personales en un bien valioso cuyo uso o comercialización constituye el principal negocio de muchas empresas[2]. Luego de observar esto, se advierte la necesidad de proporcionarles a los sujetos intervinientes en las distintas fases del cibercomercio; vigilancia, protección, confianza y seguridad.

Por otra parte, resulta que la transferencia electrónica de datos personales que se produce en la contratación electrónica, deja expuestos estos datos a una posible manipulación, en perjuicio de la intimidad de las partes[3]. A pesar de esto, las técnicas usadas en ocasión de ese proceso, sin los debidos controles y garantías, pueden introducir elementos que pongan en peligro la esfera privada y patrimonial de los

[2] La venta de datos personales de usuarios es la mayor fuente de ingresos de los portales. A cambio de una contraprestación económica, las agencias de publicidad reciben de parte de los webmasters (personas responsables de un sitio web específico) todos los datos recolectados de los registros de usuarios en estos portales. Los datos vendidos en la Web incluyen nombres, direcciones, números de pasaportes y otras informaciones financieras confidenciales como números de tarjetas de crédito, nombre de usuarios y contraseñas bancarias. Ver en http://www.proyectopyme.info/venta-datos-personales-mayor-fuente-ingresos-portales/2-13-8-13.htm.

[3] BARRIUSO RUIZ, CARLOS. (1998). *La contratación electrónica.* Madrid: Editorial Dykinson. p. 345.

intervinientes. La protección legal de los datos personales en la contratación electrónica es una protección disuasoria «a posteriori», que aunque reprima las conductas ilícitas, debe suplirse con técnicas y medidas físicas y lógicas de prevención, adoptadas diligentemente, para defender lo más posible la intimidad.

A propósito, concurren hipótesis relativas a la manera de concebir el desarrollo del comercio electrónico y el régimen jurídico de la protección de datos personales. Podemos preguntarnos, si es posible conciliar los intereses del primero con un nivel aceptable de protección de datos; o por el contrario, es posible implantar modelos de tratamiento de la información personal que cumplan con la legislación del comercio electrónico. Algunos perciben que los consumidores pueden negociar con libertad sobre su derecho a protección de datos.

En suma a todo esto, suele considerarse que la legislación de protección de datos supone un obstáculo para la expansión tecnológica y comercial y, por tanto para el comercio electrónico; incluso es considerado como una carga para las empresas. Sin embargo, una adecuada política de protección de datos puede contribuir a evitar los riesgos jurisdiccionales derivados del tratamiento y a incrementar la confianza del consumidor. Debe establecerse cuales factores determinan la sustitución de una concepción de la protección de datos como obstáculo comercial y como un simple asunto del consumidor, por una concepción de la protección de datos como ventaja comparativa en el mercado y como derecho del ciudadano.

Hoy es casi imposible, en efecto, estar en el ciberespacio sin verse confrontado con una serie de prácticas que llevan a cabo todo tipo de tratamiento de datos personales,

sin ser percibido por el usuario. Los particulares riesgos de estas actividades por parte de las empresas, exponen a los clientes a prácticas comerciales excesivas, así como a los diversos supuestos de deslealtad o licitud en la recogida de los datos, como la generación de cookies, los registros de hábitos de consulta, la combinación del catering del navegador, los hipervínculos invisibles, los webbugs, los programas espías (spyware). Todos ellos se consideran elementos vinculados con la arquitectura y configuración técnica de la red.

La generalización de prácticas de tratamiento invisible de datos personales es un buen ejemplo de la contradicción que parece mediar entre el desarrollo del comercio electrónico y el derecho de protección de datos. La configuración técnica de la red o por defecto de sus productos (software), incide determinantemente sobre el nivel general de protección de datos personales, en el entendido de que permite el tratamiento indiscriminado e invisible de éstos. Sólo deben recogerse aquellos datos que sean necesarios para la prestación de los servicios de telecomunicación, conforme a los principios de necesidad, proporcionalidad y adecuación.

Por otra parte, es público que las compañías de cibermarketing confeccionan perfiles electrónicos para distintos propósitos. En primer lugar, para el diseño de la estrategia comercial, es decir, la realización de predicciones de consumo y ventas, así como la promoción y la creación de bases de direcciones de correo electrónico que se emplean en el marketing personalizado. También para la restricción del uso de los servicios de Internet basada en la adopción de decisiones individuales automatizadas que implican la previa estratificación o segmentación socio económica de los usuarios.

En ese mismo orden de ideas, vemos como los dedicados a realizar publicidad[4] hacen uso secundario de los datos recogidos a través del tratamiento invisible para elaborar perfiles. Una vez identificado el comprador, bien porque sea él mismo quien proporcione información al conectarse al servidor, bien a través de cookies, se utiliza información previa sobre él para hacer publicidad personalizada según sus hábitos, intereses, historial de navegación. Y no se trata sólo de anuncios relacionados con los servicios y las ofertas del propietario del sitio web, sino también los emitidos por terceras partes que tienen acuerdos para apoyar el costo derivado de la gestión del servidor mediante la exposición de sus banners. En Estados Unidos, grupos de internautas como Electronic Frontier Foundation y Center for Digital Democracy han pedido al Congreso que regule las técnicas publicitarias en Internet para limitar el empleo de datos personales en la publicidad. Los citados grupos muestran su preocupación por la cantidad de datos que almacenan las compañías de sus clientes[5].

Como en Internet resulta sencillo navegar entre páginas, de tal forma que con sólo hacer "clic" en un ícono es posible dejar de visualizar una página almacenada en un

---

[4] Los paradigmas de la publicidad de Internet son las técnicas utilizadas por agencias publicitarias como DoubleClick, que permiten aislar criterios de identificación y ofrecen a los anunciantes, herramientas para dirigir a los usuarios anuncios individualizados. Esta tecnología recurre a una base de datos que contiene información acerca de millones de usuarios, con lo que se garantiza que durante las campañas publicitarias sólo se contactará con la audiencia deseada. Para lograrlo, DoubleClick recoge y trata datos personales que permiten identificar a los usuarios, describir sus hábitos y determinar en tiempo real los elementos de la población que probablemente satisfarán los criterios de los objetivos de las campañas publicitarias existentes. Luego asigna un número de identificación único a cada usuario que visita uno de los sitios Web de su red y coloca una cookie que más tarde se utilizará para identificar al usuario cuando se conecte a otro de los sitios de DoubleClick y, de acuerdo con los datos que se tengan de tal usuario, personalizar el anuncio más adecuado. Aunque el visitante no acepte la cookie se puede elaborar su perfil, sobre todo si tiene una dirección IP estática. El comercio electrónico móvil (teléfonos celulares y otros aparatos portátiles), la localización y el tráfico de datos, así como los hábitos de viaje, se pueden añadir a los datos sobre transacciones y navegación para elaborar un perfil incluso más detallado del consumidor.

[5] http://www.elpais.com/articulo/tecnologia/Grupos/internautas/reclaman/Congreso/EE/UU/medidas/proteger/privacidad/elpeputec/20090902elpeputec_2/Tes.

país para pasar a ver otra página ubicada en otro territorio; esta circunstancia hace que, en ocasiones, el usuario crea estar facilitando sus datos personales a una entidad cuando en realidad es otra (radicada probablemente en otro lugar del mundo) la que los está obteniendo, siendo muchos los casos en los que ésta última no se identifica claramente en la red.

En ese mismo orden, gran parte de los agentes que operan en el espacio cibernético y de los servidores a los que nos conectamos, se ubican en países en los que no existe legislación de protección de datos en sentido estricto (señaladamente en Estados Unidos y en Asia); el propio diseño de Internet facilita el acopio y proceso indiscriminado de información personal. Las inquietudes versan sobre ¿cómo hacer para que las empresas electrónicas cumplan la legislación?; ¿cómo proteger a los consumidores en un entorno sin fronteras, y con más énfasis, los menores?; ¿cómo minimizar los riesgos que la propia estructura tecnológica comporta para la protección de los datos personales?… Cabe advertir la inseguridad de que los datos sean interceptados durante su transmisión, sean utilizados y divulgados con fines no previstos, no autorizados o fraudulentos.

El desarrollo de la economía digital ha estimulado poderosamente el movimiento internacional de datos personales, hasta el punto de convertirse al mismo tiempo en una valiosa herramienta de todo negocio en la red y en condicionante de su desarrollo futuro. Visto que los datos personales se han convertido en objeto del tráfico comercial internacional y la existencia de paraísos de datos que buscan menores costos de tratamiento de datos, las naciones se han visto obligadas a intervenir a

través de la negociación de acuerdos de comercio bilaterales, como el Acuerdo de Puerto Seguro.

Es preciso destacar que la seguridad del comercio electrónico abarca conceptos que van más allá de la mera protección tecnológica o jurídica, como puede ser la propia fiabilidad del proveedor al que confiamos nuestros datos, las opciones que nos ofrece para dar marcha atrás ante una compra no satisfactoria o la preocupación muy extendida sobre donde irán nuestros datos y si serán revendidos a terceros sin nuestra autorización. La preocupación por la privacidad/seguridad del cliente ha demostrado tener un efecto significativo sobre la reducción en las tasas de atracción (principalmente en lo que se refiere a la intención de comprar y de compartir datos con el sitio web)[6]; constituyendo ésta circunstancia una barrera al desarrollo del comercio electrónico.

Mientras los representantes de la industria de Internet afirman que en sus plataformas es el individuo quien determina el uso de sus datos, y defienden que el marco regulador no ponga fin a la innovación, otros expertos remarcan que los derechos del interesado deben ser ampliados para que el usuario se encuentre en igualdad de condiciones respecto de la empresa. Asimismo, advierten que el detrimento de la privacidad puede desencadenar la pérdida de otros derechos y apuntan a la necesidad

[6] Ver CASTAÑEDA GARCÍA, JOSÉ A. & MONTORO RÍOS, FRANCISCO J. (2005). *La preocupación por la privacidad/seguridad como barrera al desarrollo del comercio electrónico*. Recuperado el 02 de septiembre de 2009 de http://www.revistasice.com/cmsrevistasICE/pdfs/PICE_2835_25-40__38BAF95B8EC0CD6C2481B096512DDAEA.pdf, p. 28.

de establecer un diálogo a nivel mundial sobre la privacidad para así adoptar una perspectiva global[7].

1.3 Panorama internacional de protección de datos personales.

El desarrollo legal y jurisprudencial de la acción de habeas data y de normas de protección de datos personales es una respuesta a los problemas que la informática y la telemática han ocasionado al posibilitar la acumulación de datos personales en archivos electrónicos y su posterior consulta[8]. La posibilidad de que estos datos sean incorrectos, desactualizados o caducos, así como también el poder que el conjunto de toda esta información otorga a quien la detenta, llevaron a regular estos usos con distintos enfoques.

Cabe acentuar la existencia de discrepancias muy significativas en la protección jurídica de los datos personales según el ordenamiento considerado. Podemos considerar el importante nivel de desarrollo legislativo en Europa para garantizar la protección de datos y la situación tradicional en Estados Unidos, donde ha prevalecido una aproximación caracterizada por la ausencia de intervención legislativa general, favorecedora del interés empresarial en la recopilación de datos. Pese a ello, la Unión Europea acordó con Estados Unidos un acuerdo internacional

---

[7] http://www.privacyconference2009.org/privacyconf2009/media/notas_prensa/common/pdfs/061109_2_global_privacidad_proteccion_datos.pdf

[8] PALAZZI, PABLO A. (2003). Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. En *Derecho de Internet y Telecomunicaciones*. Bogotá: Legis Editores. p. 294.

(Puerto Seguro) para permitir las transferencias internacionales de datos personales, lo cual será abordado más adelante.

En la Unión Europea, la cual se considera que ostenta el estándar de protección de datos más alto del mundo, existió siempre el consenso sobre la necesidad de que los datos personales estuvieran amparados por un marco legislativo que cubriera todos los sectores económicos y que estableciera mecanismos adecuados de protección y de sanción en caso de violación de derechos. La tutela del derecho a la privacidad en Internet se viene presentando más rígida desde la protección constitucional hasta las leyes nacionales, pasando por las disposiciones comunitarias.

Por el contrario, Estados Unidos no ha regulado en forma genérica e integral la protección de los datos personales, sino que se ha circunscripto a regulaciones sectoriales y ha preferido dejar librada tal protección a las fuerzas del mercado por medio de autorregulaciones. Esta se apoya en una serie de leyes de alcance limitado y un enfoque "caso por caso", regulando sólo sectores o industrias específicas (como la privacidad de los menores en línea[9], o las normas sobre información bancaria o la confidencialidad de los listados de videos alquilados); y sobre la jurisprudencia en materia de responsabilidad civil.

En esa misma tesitura, en Estados Unidos existen muchas barreras para el desarrollo de un sistema de protección de datos por diversos motivos. En primer lugar, su

[9] La legislación COPPA (Children's Online Privacy Protection Act) que protege la información de menores de 13 años proporcionada a través de Internet sin haber obtenido su consentimiento previo.

filosofía reguladora ha estado siempre basada en principio de mínima intervención estatal y la distribución de poderes entre las autoridades estatales y federales, cuestionándose la creación de una agencia federal de protección de datos personales. Este aspecto se manifiesta de la misma manera en las relaciones exteriores estadounidenses al extender a terceros estados su convicción de que el crecimiento del comercio electrónico ha de dejarse en manos de la iniciativa privada.

Conforme al modelo norteamericano, las normas de privacidad no pueden detener el mercado de la nueva economía. La Primera Enmienda de la Constitución Federal posee primacía sobre las reglas que limitan el uso de datos personales. Se consideran a las normas de protección de datos como barreras comerciales destinadas a proteger la industria local con el argumento de defender ciertos derechos fundamentales. Las bases de datos son fuentes importantes de beneficios que se potencian con la legalidad de su libre circulación.

Conforme al autor Víctor Drummond, en Estados Unidos el aspecto consumista de esa sociedad lleva a la necesidad de una atribución directa de responsabilidades entre las partes involucradas en la relación comercial. Así el vendedor se relaciona directamente con el comprador, con un mínimo de interferencia externa posible. O sea las políticas de privacidad entre las partes tienen un efecto que es verdaderamente regulador del mercado bajo un orden jurídico. El derecho a la privacidad está construido sobre la base de éstas, definidas entre las empresas y los consumidores a través de garantías proporcionadas por los sitios en línea.

A pesar de todo, el modelo europeo, creador de estándares internacionales de privacidad, ha tenido una gran influencia en el resto del mundo. Países como Nueva Zelanda, Hong Kong, Taiwán, Uruguay, Argentina, Australia y Canadá, han seguido en parte los patrones europeos. Otras naciones, como Polonia, Hungría, Estonia, Letonia, República Checa, Eslovaquia y Eslovenia han tenido iniciativas con el propósito de ingresar a la Unión Europea. No existen regulaciones de carácter regional en el ámbito del MERCOSUR.

A continuación, cabe mencionar que los países que no cuentan con mecanismos legales de protección de datos personales pueden verse afectados por un posible bloqueo de flujos de datos respecto de aquellos que sí cuentan con un nivel adecuado de protección. Esta circunstancia se convierte en un problema para el comercio electrónico ya que afectar la transmisión internacional de información. Por demás, se ven envueltos los intereses comerciales de las patrias envueltas. Es probable que los que no tengan leyes de protección de datos las aprueben por la necesidad de dar una respuesta a los planteos que originan las nuevas tecnologías, pero si bien esto sigue siendo un impulso para nuevas leyes, no las hace necesariamente compatibles con el molde europeo, y crea nuevamente un serio obstáculo para el libre flujo de datos internacionales y el comercio electrónico[10].

Respecto a la armonización de normas legales tendientes a proteger los datos personales, es necesaria por los siguientes motivos: a) El temor de los consumidores a concretizar operaciones comerciales en la red por la amenaza existente a su privacidad

[10] PALAZZI. Op. Cit. p. 337.

y por los perjuicios que ocasiona el empleo no ético de la tecnología; b) El deseo de las empresas de beneficiarse con toda la información que recopilan e impulsan el libre flujo de información en Internet, generando así bases para el ingreso en la nueva economía; c) La variación existente en diversos ordenamientos jurídicos acerca del tratamiento adecuado de los datos personales podría causar asimetrías.

El 6 de noviembre del 2009[11], autoridades de protección de datos de 50 países reunidas en el marco de la 31 Conferencia Internacional de Protección de Datos y Privacidad aprobaron la "Resolución de Madrid", la cual constituye la base para la elaboración de un futuro convenio universal vinculante. La resolución aprobada ofrece un conjunto de principios, derechos y obligaciones que cualquier sistema jurídico de protección de la privacidad debe esforzarse por alcanzar. Un grupo de 10 grandes empresas (Oracle, Walt Disney, Accenture, Microsoft, Google[12], Intel, Procter & Gamble, General Electric, IBM y Hewlett-Packard) han firmado una declaración en la que acogen con satisfacción esta iniciativa.

[11] https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2009/notas_prensa/common/nov/061109_estandares_internacionales.pdf.

[12] En noviembre del 2009, la empresa Google anunció el lanzamiento mundial de una nueva funcionalidad, el Panel de Control -Dashboard-, que permite a los usuarios ver, controlar y borrar toda la información vinculada a sus cuentas personales. El servicio otorga al usuario la posibilidad de conocer, de forma centralizada, qué tipo de información almacena Google de los usuarios. Ver en http://googleamericalatinablog.blogspot.com/2009/11/transparencia-y-control-ahora-con-un.html.

1.4 Derecho aplicable.

Existen diversos argumentos respecto al derecho aplicable en materia de protección de datos y comercio electrónico. En primer lugar, abordaremos la aplicación de la ley de acuerdo al lugar de recolección y almacenamiento de datos. Esto se basa en el principio de territorialidad, conforme al cual la ley que tendrá mayor vocación de ser aplicada corresponde a la del país en donde la información es almacenada por el servidor para su posterior tratamiento. Si este se reparte entre establecimientos del responsable situados en diversos estados –bien sea una sucursal o una empresa filial- cada establecimiento se rige por el ordenamiento del territorio correspondiente. Respecto al internauta, al desplazarse virtualmente es sometido a las normas del país donde los datos son recolectados.

En cierto modo, es una solución fácil y práctica de implementar, pues una oferta de servicios o productos realizada a través de un sitio web y la recolección de datos personales de los clientes por parte del proveedor de servicios u operador deberán someterse, al menos en teoría, a una sola legislación. Sin embargo, la sumisión única e irrestricta de una oferta en una página web y también la protección de los datos de los clientes que voluntariamente se desplazan y acceden en dicha página por tales ofertas, a la ley del lugar del servidor o de la zona donde el proveedor tenga su establecimiento fijo o permanente puede equivaler para los demás estados a una renuncia a una parte de su soberanía.

Es más, aplicando este criterio en forma mecánica e irrestricta, existirá el peligro de cometer fraude a la ley del país del navegante, mediante la deslocalización de los

servidores en jurisdicciones extrañas en las que no exista una adecuada protección de datos personales. Si esto se concreta con la sola finalidad de evitar los efectos de una ley nacional de orden público, entonces sería de aplicación los principios generales del derecho internacional privado, esencialmente el de prohibición de actos hechos en el extranjero para transgredir las leyes de otros países.

En segundo lugar, encontramos el supuesto de la aplicación de la ley del país desde el cual el usuario accede a la información, resultando contrario al expuesto precedentemente. Puede resultar de alguna manera inadecuado para Internet ya que implicaría que una información puesta al público o accesible desde cualquier país, deba ajustarse también a las leyes de los demás territorios donde ella es igualmente accesible.

En tercer lugar, se ha sugerido efectuar una distinción según cuál sea la política del proveedor de servicios y/o operador del sitio informático desde donde se oferta y ocurre el almacenamiento de datos personales de los clientes. Si éste adopta una política de ofertas agresivas, ya sea enviando comunicaciones no solicitadas, o instalando cookies en los ordenadores de los internautas, o efectuando tratamiento de datos personales de nacionales; las ofertas u operaciones que resulten de estas actuaciones deberán someterse a la ley del país de recepción de tal oferta o comunicación, puesto que el mismo se ha desplazado virtualmente a esa jurisdicción.

Si por el contrario, la conducta del operador del sitio web cuyo servidor almacena la información es pasiva, limitándose a colocar ofertas o contenidos a disposición de los internautas, que son los que en realidad van por ella y se trasladan virtualmente hacia

donde se alberga la información, entonces, los datos obtenidos por el operador del sitio con motivo de una transacción realizada de la manera antes descripta escapa a la legislación del lugar desde el cual el internauta accede a Internet y estará, en cambio, sometida a la del establecimiento del oferente o proveedor de servicios.

2.1 El sujeto activo: El comprador, usuario, consumidor…

El comprador es quien es quien tiene el derecho a proteger su intimidad, por lo que puede decidir cuándo, dónde y cómo se presentan y/o utilizan sus datos personales. Ahora bien, este derecho puede ser objeto de limitaciones. En Europa, la protección de datos personales tiene el rango de derecho fundamental, de ahí se deriva que puede ser limitado si hay consentimiento del titular y cuando se cumplan ciertas exigencias, fundamentalmente la necesidad y la proporcionalidad.

Como podemos observar, los clientes facilitan en una contratación electrónica datos personales como nombres, apellidos, dirección física o postal, dirección IP[13], contraseñas, número de tarjeta de crédito y su fecha de vencimiento, número de cuenta bancaria. Es importante destacar que esta operación cada vez más, se apoya en sistemas de multimedia que conjugan sonido, imagen, voz y texto. La preocupación por la privacidad/seguridad del comprador es una variable que no depende de su experiencia o habilidad en Internet[14]. El tratamiento de los datos de carácter personal requiere que el usuario sea previamente informado y de su consentimiento inequívoco, salvo las excepciones previstas por las normativas.

[13] La Unión Europea considera a la dirección IP como un dato de carácter personal.
[14] CASTAÑEDA & MONTORO. Op. Cit. p. 29.

Estas pautas resultan evidentemente aplicables al comprador en una operación de comercio electrónico, aunque se plantean ciertas dificultades, como si en dicha operación, la recogida de datos personales, es "adecuada, pertinente y no excesiva". Puede ser que no haya excesiva dificultad para argumentar la necesidad, idoneidad y proporcionalidad de la misma. Mencionamos aspectos tan diversos como el interés del vendedor de ofrecer un servicio post-venta al comprador, la necesidad de poder comunicarle eventuales vicios en el bien vendido, o finalmente, en la necesidad de documentar la realidad de ciertas operaciones a efectos fiscales.

Como hemos expuesto más arriba, si el internauta es quien ingresa libremente a un sitio, lo consulta, suscribe un servicio ofrecido, contrata un servicio o producto; puede afirmarse que adopta una conducta activa frente al sitio o servidor donde se encuentran alojadas las ofertas, los contenidos o se invita a los consumidores a ofertar. En este caso, le ofrecerá sus datos personales para finalidades determinadas y se someterá a la política de privacidad determinada por el servidor, la que a su vez deberá ser compatible con las leyes del país donde la recolección y el tratamiento de datos personales ocurren.

De otro lado, cuando un usuario completa un formulario en papel puede dudar acerca del tratamiento informático posterior de sus datos personales, pero cuando lo realiza a través de la Internet, no hay dudas respecto a su tratamiento automatizado, puesto que está la certeza de la introducción de sus datos personales en un sistema informático. Los lenguajes de programación permiten el enlace directo de los formularios de WWW con las bases de datos instaladas en el servidor, obteniéndose una integración completa entre la recogida de datos que se produce en el entorno gráfico que sirve de

interface con el usuario y la gestión en tiempo real de dicha información en la base de datos.

Conocida la oferta, el ciudadano puede decidir formular una demanda, por lo que debe suministrar datos personales al vendedor, los cuales deben estar protegidos adecuadamente en la medida en que se transmiten de forma "privada" y no "pública". Ciertamente, la transmisión de la demanda por el comprador hecha mediante mecanismos "inseguros", no hace desaparecer el deber de respeto al derecho a la intimidad informática por todos los que tengan acceso a esos datos.

El comprador puede realizar el pago del bien o servicio a través de procedimientos físicos o electrónicos. Si el pago se efectúa por medios físicos (por ejemplo, pago contra reembolso), no se plantean mayores problemas en materia de datos personales. Distinto es el supuesto de que el comprador realice el pago por medios electrónicos, bien con cargo a una tarjeta de crédito, o bien mediante una transferencia de fondos. En ambas circunstancias existen modos "seguros" o "inseguros" de efectuar la operación.

Los modos seguros se articulan en torno a la utilización de técnicas de cifrado en general (por ejemplo, para realizar operaciones de banca en línea) o de firma electrónica avanzada (que es un modo particular de cifrado). Los datos personales involucrados en la operación de pago (números de cuentas bancarias, de tarjetas, destinatarios de los pagos, etc.) se hallan protegidos por el derecho a la intimidad.

Existen páginas web que utilizan vías no seguras para la confirmación al usuario de sus propios datos de registro (incluida su contraseña de acceso) o de los datos asociados a su pedido. Son los casos en los que ésta información se remite por correo electrónico, no aplicándose en ningún caso procedimientos adicionales de cifrado, de tal forma que esos mensajes podrían ser captados y leídos por personas no identificables por el usuario. Ahora bien, el supuesto de transmisión de datos por medios "inseguros" hace extraordinariamente difícil la eventual exigencia de responsabilidades, pues el titular del derecho no puede controlar el destino de las informaciones sobre su persona que emite.

Por otro lado, en una ocasión se sostenía que la publicidad de los beneficios de la política de privacidad/seguridad compensaba la preocupación por la privacidad del cliente en Internet mediante el incremento de la propensión de éste a ceder datos personales. Sin embargo, luego de resultados empíricos demostraron que produce un efecto contrario, es decir, provoca un aumento en la preocupación por la privacidad del mismo y una reducción en la intención de ceder datos personales online[15].

Mientras tanto, en ocasiones resulta complicado para el usuario distinguir claramente la figura del comerciante (con quien realmente el primero establece la transacción comercial) de la figura de mero intermediario (que pone en contacto virtual a ambos). En este sentido, el comprador, una vez que ha facilitado sus datos personales, éstos pueden pasar por las manos de los distintos intervinientes en el proceso: el que gestiona los servidores web por cuenta del comerciante, el propio comerciante, el que

[15] Ibid. p. 31.

autoriza la transacción financiera, el que se encarga de emitir los documentos que otorgan la titularidad del producto (por ejemplo, una agencia de viajes), el que se encarga de servir el producto (logística), el que se encarga de prestar la atención al cliente[16], etc.…

2.1.1 El deber de información.

Tanto en la legislación española[17] como en la argentina[18] disponen que es lícita la obtención de datos personales del individuo en la medida en que los mismos sean "ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido". En caso de que se pretendan obtener sus datos, el sujeto debe ser previamente informado de modo "expreso, preciso e inequívoco" de lo siguiente: de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; del carácter obligatorio o facultativo a las preguntas que les sean planteadas; consecuencias de la obtención de los datos o de la negativa a facilitarlos; posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición de datos; y, de la identidad y dirección del responsable del tratamiento o en su caso, de su

---

[16] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2000). *Recomendaciones al sector del Comercio electrónico, para la adecuación de su funcionamiento a la ley orgánica 15/1999, de 13 de diciembre de 2000, de protección de Datos de Carácter Personal*. Recuperado el 01 de septiembre de 2009, de https://www.a gpd.es/portalweb/canaldocumentacion/recomendaciones/index-idesidphp.php# 0103. p. 4.

[17] Artículos 4 (Calidad de los datos) y 5 (Derecho de información en la recogida) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, España.

[18] Artículos 4 (Calidad de los datos) y 6 (Información) de la Ley 25.326, Protección de los Datos Personales, Argentina.

representante, en caso de que se violentara o desconociera algunos de los principios generales antes mencionados.

También ambas normas disponen que los datos obtenidos no puedan usarse para finalidades incompatibles con aquellas para las que éstos hubieran sido recogidos. Estos datos deben almacenarse de forma que se garantice el "derecho de acceso" y serán "exactos", debiéndose rectificar en caso contrario. Podrán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que hubieren sido recabados. Está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos.

La Agencia Española de Protección de Datos (en lo adelante, AEPD) recomienda[19] que, desde que se recaben datos de carácter personal, se incluirá claramente visible la información a la que hace referencia el artículo 5 de la de la Ley Orgánica 15/1999, de 13 de diciembre, que el usuario deberá poder obtener con facilidad y de forma directa y permanente. También podrá optarse por incorporarse en la página web un texto o un botón etiquetado que, al ser seleccionado mediante un "click" permita obtener la citada información. No obstante, considera más adecuada una opción según la cual la lectura de dicha información se presente como ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos a la entidad que los está recabando.

---

[19] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Recomendaciones al sector del Comercio electrónico, para la adecuación de su funcionamiento a la ley orgánica 15/1999, de 13 de diciembre de 2000, de protección de Datos de Carácter Personal*. Op. Cit. p. 10.

Asimismo, tanto el referido artículo 5 como la AEPD instituyen que cuando el responsable no se encuentre establecido en el territorio de la Unión Europea y se sirva en el tratamiento de datos de medios situados en el territorio español le incumbirá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España. En todo caso, la información deberá proporcionarse en el mismo idioma en que se recaban los datos personales.

Con todo, el ciudadano le corresponde quedar informado por completo acerca de los usos concretos que se realizarán de sus datos personales. En caso contrario, se produciría una vulneración del principio de finalidad en el tratamiento de los datos. Además el usuario deberá estar convenientemente informado en todo caso del momento en que desde una página web se transfiere el control a otra, de tal forma que no pueda albergar dudas al respecto.

2.1.2 El consentimiento informado.

Las legislaciones relativas a protección de datos personales obligan a que la obtención de los mismos se produzca con el consentimiento informado del interesado. Estos no podrán usarse para finalidades incompatibles con aquella que ha justificado su recogida. En este sentido, para que tales datos puedan ser manejados con una finalidad no compatible con ésta, es imprescindible obtener previamente el consentimiento inequívoco del afectado.

Con motivo de esto, las empresas para recabar este consentimiento en Internet, necesitan un procedimiento en el que el usuario ostente una participación activa, de tal

forma que, a través de la red informática, pueda manifestar su voluntad en uno u otro sentido. Pueden introducir en todos los formularios electrónicos[20] cláusulas de consentimiento respecto al tratamiento automatizado de los datos personales introducidos, así como información sobre la posibilidad de modificar o incluso cancelar los registros referentes a su persona.

La AEPD ha resuelto que cuando un usuario facilita voluntariamente sus datos de carácter personal a través de Internet para una finalidad distinta de la mera ejecución de la transacción comercial, se entenderá que consiente en el tratamiento de los mismos en los términos de los que ha sido convenientemente informado en el momento de la recogida. En caso de que el afectado haya revocado su consentimiento para el tratamiento, el responsable de la base de datos fichero habilitará los medios oportunos para la exclusión.

Los "clip wrap agreements" o "point and click agreements" son contratos usados habitualmente en el comercio electrónico, que basan su validez en el acto de pulsar el botón de aceptación por parte del usuario. Su dificultad estriba en que no existe una firma o una muestra de consentimiento que se conserve como prueba de la aceptación del usuario. No obstante la mayoría de las transacciones electrónicas que se realizan en la actualidad se basan en acuerdos que se aceptan pulsando un botón de una página web, por lo que, con el tiempo, se aceptará esta vía cuando se cumplan con los requisitos necesarios para ello.

[20] Estas casillas, según lo dispuesto por la Directiva Europea sobre Comunicaciones Comerciales deben estar en blanco para que sea el propio afectado el que las marque si desea recibir tal información y porque tal acto supone el consentimiento expreso.

Como ya hemos mencionado anteriormente, al realizar una operación de cibercomercio, se obtienen ciertas informaciones del sujeto sin su consentimiento y sin que esté acreditada su necesidad y proporcionalidad. Por ejemplo, la posibilidad de introducir unos archivos llamados "cookies" al visitar un determinado sitio. Esta problemática será abordada más adelante.

En otro entorno, existen compañías pertenecientes a grandes grupos empresariales que comparten su cartera de clientes con las demás empresas de su grupo, por lo que en su propio espacio web incluyen cláusulas informativas con las que pretenden cubrir el requisito legal del previo consentimiento del interesado. Las fórmulas manejadas suelen consistir en una referencia a la "posible cesión de datos a otras empresas del grupo", en orden a que tales datos sean utilizados con la finalidad de remitir "informaciones comerciales de su interés".

Sin embargo, es precisamente la diversidad de actividades que pueden coincidir en un mismo grupo lo que puede introducir un elemento de inseguridad en perjuicio del ciudadano, especialmente en casos en los que está formado por un gran número de compañías. De esto se deduce, que el grupo empresarial puede llegar a manejar una información muy completa acerca de los hábitos de las personas con las que las compañías participadas han establecido una relación comercial, circunstancia ésta de la que quizás no sean del todo conscientes los compradores / usuarios.

En la práctica, una vez que el titular ha proporcionado sus datos a un sitio web, sus datos pueden ser fácilmente utilizados por dicho sitio y/o cedidos a terceros para un uso diferente para el que se habrían requerido. Por ello, toda cesión de datos a

terceros, así como toda utilización diferente de aquella para la cual se habrían solicitado los datos debería contar con el consentimiento expreso del titular.

2.1.3 Alternativas del sujeto activo.

La gran mayoría de las compañías han creado distintas vías para facilitar al ciudadano el ejercicio de los derechos que las regulaciones de protección de datos personales le reconocen. Dado que la propia naturaleza de Internet permite una interrelación fácil y rápida entre comprador y vendedor, generalmente se ha utilizado la vía del correo electrónico como fundamental tanto para canalizar las solicitudes de acceso, rectificación, oposición y cancelación, como para remitir las consiguientes contestaciones por parte del responsable del fichero[21].

Aparte de esto, muchas entidades han habilitado en su página electrónica un espacio que permite al interesado, consultar fácilmente los datos que figuran en su fichero, para lo que se solicita previamente al usuario se identifique y que se autentique su identidad a través de la contraseña que eligió al momento de registrarse. Esta vía le facilita considerablemente el ejercicio de su derecho de acceso e introduce un mayor nivel de transparencia por parte del responsable del fichero. Por demás, también ofrecen las vías de comunicación telefónica (servicio de atención específico) y la comunicación postal.

---

[21] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2000). *Recomendaciones al sector del Comercio electrónico, para la adecuación de su funcionamiento a la ley orgánica 15/1999, de 13 de diciembre de 2000, de protección de Datos de Carácter Personal*. Op. Cit. p. 7

La confianza del cliente en la empresa se ha erigido como un importante factor compensador del efecto negativo que constituye la preocupación por la privacidad/ seguridad en el comercio electrónico. Dicha confianza constituye un factor importante para conseguir superar la barrera. Existen entidades independientes privadas garantes de la protección de la privacidad/seguridad, que emiten certificados de seguridad sobre la privacidad de los usuarios, pretendiendo reducir la preocupación de éstos, lo que favorece el desarrollo del comercio electrónico. Podemos mencionar a Confianza Online en España, Trust-e en Estados Unidos, Fundación Vanzolini en Brasil. La tendencia es que las empresas se asocien a dichas organizaciones.

Por otro lado, para que exista una operación de comercio electrónico "segura", como hemos mencionado el comprador le conviene formular su demanda mediante procedimientos que impidan el acceso a esos datos por personas no identificables, como las técnicas de encriptación, firma digital. De tal forma, los datos personales son cifrados por el consumidor, de suerte que sólo puedan ser descifrados por quienes tengan acceso a las claves correspondientes. También debe que se utilicen servidores seguros: con sistema SSL y el protocolo https, donde los datos viajan encriptados hacia su destino.

2.2 Los sujetos pasivos: el vendedor, el servidor y el certificador.

Son muchos los agentes que intervienen en el procesamiento de datos personales y el negocio electrónico. Entre estos se encuentran el proveedor de servicios, el vendedor y, eventualmente, el certificador de la identidad del comprador o del vendedor. Estos se encuentran sometidos a ciertos deberes generales para con el sujeto activo del

derecho a la intimidad informática. De esta multiplicidad de posibles responsables de los ficheros deriva el problema de la segmentación de roles a efectos del tratamiento de los datos. Muchos de ellos desempeñan en la práctica funciones que jurídicamente están divididas. Algunos servidores de Internet operan a un mismo tiempo, en calidad de proveedores de acceso, proveedores de contenido, buscadores, portales, servicios de correo electrónico u otros servicios de valor añadido como la elaboración de estadísticas de navegación o visitas.

2.2.1 El vendedor.

Una vez que el comprador ha formulado su solicitud de un bien o servicio aceptando la oferta que se le ha hecho, el vendedor obtiene toda una serie de datos personales de éste. El comprador normalmente no creará un fichero de datos personales, pero el vendedor sí. Existen argumentos de necesidad y proporcionalidad, relacionadas con la adecuada prestación del servicio para que el vendedor normalmente archive estos datos personales. Por un lado, éstos son necesarios para una adecuada prestación del bien o servicio y, por otro lado, en caso de eventuales reclamaciones de responsabilidad (por ejemplo, si el vendedor entrega el bien o presta el servicio antes de comprobar si en la cuenta bancaria del comprador existen fondos).

Las empresas vendedoras generalmente restringen su actividad a las tareas como la atención telefónica, las operaciones logísticas o los servicios informáticos. Además existen casos en que los servicios informáticos se prestan por compañías extranjeras establecidas en otros países del mundo, cuyas condiciones aplicables a la prestación

del servicio se recogen en un documento – tipo, que utiliza habitualmente el prestador y cuya redacción, a veces, no se adapta a las legislaciones de los países donde operan.

Las legislaciones de protección de datos personales, en su generalidad, les imponen a las empresas dos grupos de obligaciones: unas afectan a su relación externa con los clientes (información, consentimiento, transparencia, ejercicio de derechos…), otras a su propia organización interna (medidas de seguridad, relaciones con la autoridad de protección de datos correspondiente). Las empresas sólo pueden crear un fichero de datos personales cuando ello sea necesario para el logro de su actividad y se respeten las garantías establecidas por sus correspondientes normativas, las cuales consagran lo siguiente:

- *Deberes de información en la recogida de datos*: Como ya ha sido expuesto, le corresponde a la empresa informar al comprador lo siguiente:

  a) La existencia de un fichero o tratamiento de datos de carácter personal.

  b) La finalidad y destino, por ejemplo, cuando los datos vayan a ser utilizados para segmentación o categorización con fines comerciales, recogen tanto para firmar un contrato (suscripción de Internet, pedido de un producto, etc.).

  c) Si los datos solicitados son obligatorios u opcionales, ya que la información obligatoria es aquella necesaria para prestar el servicio solicitado. La naturaleza obligatoria u opcional se podría indicar, por ejemplo, mediante un asterisco junto a los datos obligados o bien añadiendo la palabra "opcional" junto a la información no obligatoria. Si el interesado no facilita la información opcional no puede utilizarse en su contra de ninguna manera.

  d) De las consecuencias de la obtención de los datos o de la negativa a facilitarlos.

e) De la posibilidad de ejercitar los derechos del titular de los datos (objeción, acceso, rectificación, cancelación) y de las condiciones para su ejercicio. Puede ser en línea, por ejemplo, mediante una casilla que el usuario puede marcar para oponerse a que sus datos sean cedidos o tratados para determinados fines. Es posible proporcionar el nombre y la dirección (postal y/o electrónica) del servicio o la persona encargada de responder a las preguntas relacionadas con la protección de datos.

f) De la identidad y dirección del responsable del tratamiento o en su caso, de su representante. Por demás, es preciso declarar estas informaciones en la página electrónica de la empresa.

- *Deberes de notificación y registro ante las agencias de protección de datos correspondientes*: La notificación contendrá, entre otros aspectos, quien es el responsable del fichero, finalidad del mismo, ubicación, tipo de datos personales que contiene, medidas de seguridad y cesiones de datos personales que se prevean realizar.

- *Deberes de integridad y seguridad*[22]: Una vez creada la base de datos, su responsable y, en su caso, el encargado de su tratamiento, deben adoptar las

[22] El Departamento de Comercio de Estados Unidos de América promulga un plan de seguridad de datos personales basado en cinco principios claves: a) Conozca su inventario: Sepa cuál es la información personal que usted posee en sus archivos y computadoras; b) Reduzca sus archivos: Mantenga únicamente la información que necesita para manejar su negocio; c) Cierre con llave. Proteja la información que mantiene bajo su cuidado; d) Elimine lo innecesario: Deseche correctamente la información que ya no necesita; e) Planifique con anticipación. Elabore un plan para responder a los incidentes de seguridad. Los cuatro elementos claves que un plan de seguridad debe contener son: seguridad física, seguridad electrónica, capacitación del personal y prácticas de seguridad de los contratistas y proveedores de servicios.

medidas de índole técnicas y organizativas necesarias que aseguren la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Cabe mencionar las medidas de seguridad que garantizan la autenticidad del sitio web, la integridad y la confidencialidad de la información transmitida a través de la red electrónica, fundamentalmente cuando entre ellos figura la identificación de la tarjeta de pago. También puede usar procedimientos de cifrado para hacer más seguras sus operaciones.

- *Deber de secreto*: Tanto el responsable de la base de datos como todos los que intervengan en cualquier fase del tratamiento quedan obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Estas obligaciones subsisten aún después de culminar sus relaciones con el titular del fichero o, en su caso, con su responsable. Su vulneración puede acarrear responsabilidad civil y penal, así como sanciones.

- *Deber de comunicación de cesión a terceros*: El responsable del fichero debe comunicar al sujeto activo la primera cesión que lleve a cabo de los datos personales de este último, indicando asimismo la finalidad, la naturaleza de los datos cedidos y el nombre y dirección del cesionario. De esta obligación está exento el sujeto pasivo en una serie de supuestos: a) que la cesión sea consecuencia necesaria de una relación jurídica libremente aceptada por el titular de los datos y se limite a la finalidad que justifique la cesión; b) que la comunicación de los datos se haga a una serie de órganos públicos, en tanto actúen en el ejercicio de sus funciones; c) que los datos transmitidos hayan sido objeto de "disociación", de suerte que no pueda inferirse a qué persona se refieren.

Hay que indicar si se comunicarán o pondrán a disposición de terceros, en particular socios empresariales, filiales, etc., y para qué fines (aquellos distintos de prestar el servicio solicitado y de marketing directo).

Como se advierte, estos deberes legales inciden tanto en la organización interna como en las relaciones de las empresas con sus clientes (actuales o potenciales). Además las empresas pueden instrumentalizar el derecho de protección de datos personales a través de las políticas de privacidad y los sellos de calidad; esto con el propósito de aumentar la confianza en el comprador y contribuir al desarrollo del comercio electrónico. Debido al costo que acarrea una violación del sistema de datos personales, la pérdida de confianza de sus clientes y quizás hasta tener que asumir los costos de su defensa en una demanda judicial, proteger la información personal es simplemente una cuestión de buen sentido comercial.

Cabe preguntarse si existe algún tipo de relación entre el nivel de protección de datos que ofrece una empresa online y su ratio de ventas o su volumen de negocios. El grado de protección de la información personal que proporcionan las empresas electrónicas parece ser independiente respecto de su volumen de negocio. Esta aparente contradicción se explica por la escasa conciencia ciudadana sobre el derecho de protección de datos.

Respecto al tratamiento invisible de datos personales, la empresa debe informar con claridad de la existencia de métodos automáticos de recogida de datos, antes de emplearlos, si es posible, en su política de privacidad de datos personales. Cuando éstos sean utilizados, el usuario debe recibir la información correspondiente. En

especial, si en la página web se localizan banners de compañías de cibermarketing, las cuales financian dichas páginas, que recopilan así datos personales. Se puede por ejemplo, introducir un apartado en la política de privacidad en el que se informe del nombre de dominio del servidor, la finalidad de las cookies, su plazo de validez, y si es necesaria o no la aceptación de las mismas para visitar el sitio, y según el caso, la opción de oponerse a su uso, o las consecuencias de desactivar dichos procedimientos.

Asimismo la información y la posibilidad de oponerse a la recogida deberán comunicarse antes de utilizar cualquier procedimiento automático que desencadene la conexión del ordenador del usuario con otro sitio Web, por ejemplo, cuando un sitio web conecta automáticamente al usuario a otro sitio para mostrarle la publicidad en forma de pancarta, con el fin de evitar que este segundo sitio recopile datos sin que el usuario sea consciente de ello.

Por otra parte, en algunas tiendas en línea no se identifica explícitamente al responsable del fichero o tratamiento, situación ésta que coloca al afectado en indefensión respecto al ejercicio de sus derechos, puesto que, dicha figura jurídica no siempre coincide con la de la entidad o persona que ha registrado el dominio en Internet. Esto se agrava especialmente en aquellos casos en que el usuario accede a una página a través de un hiperenlace.

Respecto a la entrega del bien o la prestación de servicios por parte del vendedor, éstas pueden ser físicas o electrónicas, y a la vez puede hacerse por medios seguros o inseguros. En el caso de entrega o prestación física, se precisan ciertos datos personales del destinatario del bien o servicio (por ejemplo, la dirección del

domicilio); en el supuesto de entrega o prestación electrónica nos encontramos nuevamente con el problema del modo seguro o inseguro de realización de la obligación.

En ese sentido, la entrega de un bien electrónico (por ejemplo, descargas en línea de un programa de ordenador, un archivo musical, un archivo de texto, una obra literaria, un video) precisa de una serie de datos personales del destinatario (dirección IP del ordenador, dirección de correo electrónico, fundamentalmente). Si de lo que se trata es de la prestación de un servicio electrónico en línea (asesoramiento jurídico, económico-fiscal, psicoterapia, etc.) esa necesidad de datos personales es aún más visible.

Es considerado por la AEPD una buena práctica que se facilite y permita la consulta anónima de sitios comerciales sin solicitar a los usuarios que se identifiquen mediante su nombre, apellidos, dirección electrónica u otros datos. En adición a esto, las empresas deberían someterse anualmente a auditorías[23] de protección de datos personales realizadas por entidades como BBB Online, Webtrust, Trust–e. Estas auditorías no se han establecido como obligatorias con el fin de no desincentivar a las pequeñas y medianas empresas a adherirse a los principios de protección de datos personales.

[23] Podemos observar claramente el caso de la empresa de procesamiento de datos Choicepoint, la cual fue multada por el Departamento de Comercio de los Estados Unidos por no haber protegido adecuadamente los datos confidenciales de sus clientes, ya que mantuvo apagado su programa de seguridad por cuatro meses.

2.2.2 El servidor.

Los operadores que presten servicios y/o exploten redes de telecomunicaciones, al público, están obligados a respetar el derecho a la intimidad. Estos pueden almacenar automática, provisional y transitoriamente los datos transmitidos siempre que dicho almacenamiento sirvan exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión.

A los efectos del tratamiento de datos personales, tanto en Argentina[24] como en España[25], cuando se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos. No obstante a ello, en Argentina se prevé que si en caso de que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

En Estados Unidos existe una política de libertad y de no responsabilizar a los proveedores de servicios de Internet. Igual acontece, en la Unión Europea, la cual en

---

[24] Artículo 25 (Prestación de servicios informatizados de datos personales) de la Ley 25.326, Protección de los Datos Personales, Argentina.
[25] Artículo 12 (Acceso a los datos por cuenta de terceros) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, España.

su Directiva 2000/31/CE, establece la inexistencia de obligación general de supervisión.

2.2.3 El certificador.

La criptografía u ocultamiento de la información y dentro de ésta, los sistemas de clave pública asimétrica, las medidas de seguridad y sellamiento, los códigos, las claves, los sistemas biométricos, etc., dan respuesta hoy a la protección preventiva de datos personales, vedando su uso a quienes no van dirigidos. Durante la transmisión de éstos, la ausencia de una protección de cifrado provocaría que cualquier persona pudiese interceptarlos y utilizarlos para su propio lucro.

Un programa "firewall" facilita los accesos al servicio con autenticación, y es capaz de impedir el acceso a la red de determinados tráficos maliciosos (por ejemplo, como hackers). En este terreno, el phishing está socavando la confianza de algunos usuarios, ya que el perfeccionamiento de las falsificaciones de sitios web puede llevar fácilmente al engaño. Los certificados digitales suministrados por autoridades de certificación evitan la suplantación de identidades y la falsificación.

El proveedor de servicios de certificación de la firma electrónica goza de unos específicos deberes de protección de datos. Por ejemplo, la Unión Europea establece que los Estados miembros velarán por que éstos cumplan con las exigencias que en materia de protección de datos se han establecido, y sólo puedan recabar datos personales si concurren las principios de necesidad y consentimiento del titular,

directamente de éste, y solo hasta donde sea necesario para la finalidad de emitir un certificado. Los datos no pueden ser procesados con otros propósitos.

En Argentina[26], son obligaciones del certificador licenciado cumplir con las normas y recaudos establecidos para la protección de datos; recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional; mantener la confidencialidad de toda información que no figure en el certificado digital.

El certificador, a solicitud del firmante, puede indicar un seudónimo en vez del nombre del solicitante en el certificado. Este puede transmitir los datos relativos a la identidad del firmante a las autoridades públicas que lo requieran con su consentimiento. Si esto no puede ser obtenido porque la transferencia de los datos que revelan la identidad del afectado es necesaria para la investigación de delitos criminales graves, la transferencia se conservará y el afectado será informado tan pronto como sea posible después de que la investigación haya sido completada.

[26] Artículo 21 de la Ley Nº 25.506, Firma Digital, Argentina; artículo 34 del Decreto 2628/2002, reglamentario de la ley de Firma Digital.

3.1 Las galletas informáticas "cookies".

Los perfiles de consumidores obtenibles de una fuente potencialmente tan rica de información como es la Internet -a través del uso de mecanismos como el de las cookies-, han pasado a constituir un importante, poderoso y apreciado bien que permite a las empresas que prestan servicios en línea diferenciarse a nivel internacional de sus competidores al poder realizar ofertas que tiendan a acercarse cada vez más a los hábitos, deseos o necesidades de los consumidores actuales o potenciales.

La posterior utilización de los datos personales recolectados y almacenados por las cookies es un problema propio de las empresas que practican el comercio electrónico. Cuando se efectúa una compra o cualquier otro negocio en la red, el usuario proporciona voluntariamente datos personales, los cuales inmediatamente son integrados de manera automática a una misma base de datos con otras informaciones recogidas a través de las cookies. De este cruce de datos resulta un perfil completo del usuario y la posibilidad de su comercialización.

Los puntos centrales del debate se sitúan entre la protección de la privacidad de los navegantes de Internet, quienes rechazan ser monitoreados por los comerciantes virtuales, y del otro lado, las empresas ".com", empujadas por el libre comercio, aducen que estos cambios estimularían nuevos aumentos en los costos de operaciones

de las transacciones electrónicas. En ese mismo orden, el problema de las cookies alcanza la polémica cuestión del movimiento transfronterizo de datos personales.

Las galletas informáticas o cookies, como se les denominan frecuentemente, son pequeños ficheros de datos que operan en dos fases. En la primera, se generan a través de las instrucciones que los servidores web envían a los programas navegadores, guardándose en un directorio específico del ordenador del usuario. Luego, y esto es lo más incierto, son transferidas automática y clandestinamente (esto es, sin el consentimiento del usuario) por el servidor que las generó en el momento en que el ordenador del usuario visite cualquier página de ese servidor.

También las cookies se definen como técnicas que ofrecen las nuevas tecnologías que vienen a suplir lo que la contratación electrónica, esto es, la presencia física simultánea de los contratantes, resta frente a la contratación convencional en la que el prestador de servicios ve, conoce y orienta en la compra o la prestación de un servicio por el consumidor o usuario[27]. Si bien hay distintos tipos de cookies, nos concentraremos en las remanentes y de sesión.

Las cookies remanentes permiten recolectar información voluntariamente dada por el titular de los datos, pero también otros datos agrupados o asociados de una manera mucho más discreta, como ocurre cuando se detectan las últimas páginas consultadas, el resultado de un chat o conversación del internauta o el perfil técnico del visitante. Son independientes de la dirección IP: ellos marcan una máquina y no una conexión.

[27] ARIAS POU, MARÍA. (2006). *Manual Práctico de Comercio Electrónico,* Madrid: La Ley. p. 276.

Si una dirección IP cambia entre dos conexiones, la cookie hace el vínculo entre una y otra, salvo que éste sea destruido por el utilizador.

Por otro lado, las cookies de sesión se autodestruyen cuando el visitante abandona el sitio elegido. Hay sitios interactivos que necesitan utilizarlas bajo pena de no poder funcionar. Las remanentes tienen una duración más prolongada que fija unilateralmente la persona que las programa.

Las herramientas informáticas que estamos analizando, registran los sitios a los que el usuario va ingresando, creando así una imagen del mismo sobre sus preferencias de navegación, los lugares que visita habitualmente; predicen las necesidades, gustos y apariencias; y aprenden de las propias reacciones de los usuarios. Además realizan entrecruzamiento o asociación de datos personales obtenidos de distintas fuentes. Su admisibilidad en el marco de la normativa sobre protección de datos puede plantear notables dificultades. Parte de la doctrina consideran ilegal su emisión, por lo que han reclamado su prohibición por considerarlas una invasión a la privacidad.

Desde la otra vereda, quienes defienden el uso de éstas técnicas entienden que la prohibición atentará contra el desarrollo comercial en Internet. Esto debido a que pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo, para analizar la efectividad del diseño y de la publicidad de un sitio web; para verificar la identidad de usuarios partícipes en una transacción en línea; facilitar el suministro de servicios de la sociedad de la información, recordando las preferencias del usuario en su navegación habitual por la red, lo que facilita una mayor celeridad en la conexión. Quienes las emplean habitualmente suelen argumentar que el usuario siempre tiene la

posibilidad de desactivar en su programa navegador la opción que le permite recibirlas o configurarlo para que le avise cada vez que se intenta enviarle una.

En Estados Unidos como no se reconoce la eficacia del derecho a la intimidad informática entre los particulares, las cookies pueden tener cabida legal. En Europa[28], más concretamente en España, la utilización de esta técnica vulnera el derecho a la protección de los datos pues, no sólo no se trata de una actuación necesaria y proporcionada, sino que además el usuario no es informado de ello. Sin embargo, hay una tendencia universal[29], a considerar el tratamiento ilícito de datos personales a través de la utilización de las cookies, como una violación de la privacidad.

En la República Argentina, no existe ninguna normativa referente al uso de las cookies. En ese caso, se recurre a la aplicación del supuesto del artículo 27 apartado 1 de la ley 25.326 de Protección de Datos Personales, que establece que en la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promociónales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al

[28] En noviembre del año 2009, el Consejo de la Unión Europea aprobó una ley que requiere que los usuarios de Internet otorguen su consentimiento explícito ante las cookies. Con esta nueva regulación lo que se pretende es modificar lo dispuesto en la Directiva sobre la privacidad y las comunicaciones electrónicas aprobada en el año 2002 y en la Ley de Servicios de Sociedad de la Información y Comercio Electrónico. De acuerdo con esta ley para la utilización de cookies es necesario informar a los usuarios de manera clara y completa sobre su utilización y finalidad, así como, ofrecerles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito. Ver en http://www.aecem.org/detalle_contenido.html?ver_id=20528.

[29] En Estados Unidos, las políticas de privacidad tienden a rechazar la utilización de datos personales e informaciones para fines distintos a los determinados e indicados en el momento de su recogida, aunque muchas veces en la práctica las empresas no actúen de esa forma.

público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

Por demás, la situación de los responsables por la instalación de cookies deberá ser apreciada en función de circunstancias tales como: si éstos disponen de otras informaciones con las cuales puedan cruzar datos o informaciones; las características técnicas o funcionamiento de su sistema de cookies; la naturaleza de la información que éstos recolectan y almacenan; la finalidad que persiguen mediante su tratamiento. Para determinar si se produce una intromisión a la intimidad del usuario, es preciso cerciorarse de los siguientes aspectos:

a) *Contenido*: Las cookies pueden contener datos personales o cualquier otro tipo de información relacionada con la relación cliente-servidor. Si el contenido está compuesto por datos que son necesarios para efectuar transacciones cliente-servidor, en las que no se gestiona información relativa a personas físicas, no existe lesión potencial de la intimidad.

b) *Asociación de los datos a una persona identificada o identificable*: Algunos programas navegadores asignan de forma automática el nombre del usuario al archivo que se genera como cookie. De esta manera, el nombre del fichero puede estar formado por el nombre del usuario, un símbolo de separación y el nombre del servidor que ha dado instrucciones para generar el archivo cookie. Para que esta asignación pueda producirse, el navegador debe haber sido previamente personalizado por el usuario, en el momento de la instalación o con posterioridad. En muchos casos esa configuración viene predeterminada en el sistema. Si ello no

se produce, el contenido del cookie no podrá ser considerado como personal, ya que no podrá ser asociado a una persona identificada.

En principio no se estaría transgrediendo las normas de protección de datos si se recurre al empleo de una cookie, con independencia de todo otro medio de identificación y pretendiéndose con ello simplemente marcar una computadora. En este supuesto, las informaciones se almacenarían sobre el disco duro y serían transmitidas al servidor web que ha colocado las cookies cada vez que el ordenador del internauta se reconecte con el sitio en cuestión independientemente de la persona física que esté usando la computadora.

No obstante, el archivo cookie puede contener la dirección IP del usuario. En ese caso su identidad podría ser obtenida si utiliza una IP fija, siempre que sea notorio su uso por un usuario determinado. En el caso de las IP dinámicas o cambiantes, la única forma de obtener la identidad del usuario sería mediante requerimiento judicial al proveedor de servicios que le dio acceso a la red, antes de que los datos de la sesión desaparezcan del listado de operaciones del servidor. Las dificultades inherentes a este sistema de identificación, según Javier Rivas Alejandro[30], hacen pensar que la inclusión de una IP dinámica no es suficiente para considerar el contenido como datos de carácter personal.

[30] RIBAS ALEJANDRO, JAVIER. (1999). *Aspectos jurídicos del comercio electrónico en Internet.* Pamplona: Editorial Aranzandi. p. 51.

Las leyes de protección de datos no permiten la asociación entre la información recopilada y tratada con su titular. Por tal razón, las empresas electrónicas que recurran al uso de cookies, deben utilizar métodos de disociación de datos adecuados para evitar la identificación del internauta a la hora de recolectar datos personales. Si las cookies permiten individualizar al titular de los datos personales, y por ejemplo, se recaba información del internauta que permite predecir sus hábitos de consumo, es muy probable que en la práctica el operador del sitio o proveedor de servicios infrinja el principio de finalidad y/o proporcionalidad.

c) *Consentimiento del usuario*: Puesto que el derecho a la protección de datos es renunciable, el usuario que mantenga una relación negocial con el propietario del servidor, puede autorizarle contractualmente para que obtenga la información necesaria para concretar su oferta o para mejorar el servicio con prestaciones adicionales. En este caso, a la tradicional cláusula contractual por la que se autoriza el tratamiento automatizado de sus datos personales debe añadirse la figura de la cookie, como instrumento para obtener datos adicionales acerca de los hábitos de consumo, frecuencias de visita de una sección determinada, tipo de noticias a suministrar, etc.

También puede obtenerse una autorización implícita mediante la advertencia de que el sitio web hace uso de éstos mecanismos informáticos, y que le es permitido al usuario impedir el acceso a su ordenador, mediante la opción correspondiente de su navegador. Si la página visitada tiene una sección que informa sobre las funciones y finalidades de la cookie, y el usuario puede comprobar su carácter

inofensivo, es probable que autorice su entrada en el sistema. En especial, si la recepción de la cookie es un requisito previo para la visualización de la página y ésta contiene algo que le interesa, por ejemplo, los servidores de cuentas gratuitas de correo electrónico.

d) *Función*: Esta es necesaria para poder valorar si se ajusta o no al derecho. Consiste en informar acerca de la utilización de las cookies en la configuración del navegador, especificando claramente su finalidad, así como también si incluye la realización de tareas de marketing o de creación de bases que pueden ser transferidas a terceros. La utilización posterior de los datos personales almacenados puede generar una violación de la privacidad de los titulares de los datos. Este sería el único caso, en que la instalación de la cookie y posterior utilización de la información es totalmente lícita, ya que el usuario ha aceptado no sólo su instalación, sino que también ha autorizado el libre uso de la información.

   En caso contrario, es decir, si la información es obtenida sin el respectivo consentimiento pueden surgir conflictos con las normativas de protección de datos. En ese sentido, existe la posibilidad de declarar ilícitos los contenidos activos, es decir aquellos que no se limitan a ser un fichero de datos sino que pueden ser ejecutados de forma no consentida, obteniendo mayor información. Javier Rivas Alejandro se refiere a los apples de Java y Controles ActiveX que se instalan en el disco duro del ordenador y comprueban los datos personales que

figuran en el ordenador del usuario, aprovechando la existencia de otros cookies que pueden revelar sus gustos o preferencias[31].

Ahora bien, a través de la Política de Privacidad de Datos Personales, debe comunicárseles a los usuarios cuáles son los datos personales que serán recopilados, qué destino se les darán y si se compartirán con terceros, para permitir una aceptación libre, expresa e informada. Además, en los supuestos de aceptación, siempre conviene ofrecer al usuario que la recibe la posibilidad de solicitar en cualquier momento que sus datos personales sean excluidos del fichero en el que hayan sido incorporados, mediante un procedimiento sencillo y gratuito.

Sin embargo, lo expuesto en el párrafo anterior, no es necesario, de un lado si los prestadores proceden a almacenar esa información para efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas; y de otro lado, cuando el almacenamiento de esa información sea estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

[31] Ibid. p. 52.

3.2 Comunicaciones comerciales no solicitadas.

El concepto de dato personal comprende cualquier información concerniente a persona física identificada o identificable, lo que requiere la convergencia de dos elementos: por una parte la existencia de un dato y de otra, que dicho dato pueda vincularse a una persona identificada o identificable. En el supuesto de direcciones electrónicas, la información está constituida por un conjunto de signos o palabras que la diferencian de las demás, siendo el titular de la misma quien generalmente decide y elige la dirección correspondiente, con el único límite de que no exista otra dirección idéntica correspondiente a otro titular.

En ese mismo sentido, en la selección de la dirección electrónica se pueden elegir combinaciones que no contengan significado alguno o, incluso, utilizar como combinación el nombre de la persona o algún otro dato identificativo, como la organización donde trabaja o a la que pertenece una persona, lo que puede ser de gran interés para una empresa publicitaria. Esta vinculación directa o indirecta con una persona física la convierte en un dato de carácter personal. La AEPD considera la dirección de correo electrónico como un dato personal y por consiguiente, su tratamiento estaría incluido en el ámbito normativo de la protección de datos personales.

El hecho de que una dirección electrónica se exteriorice de forma voluntaria por el usuario, no quiere decir que este dato esté disponible para cualquiera, sino que únicamente y por regla general, estará disponible y será conocido por aquellos a quienes voluntariamente se lo indique el titular de ella. En consecuencia las empresas

o entidades públicas o privadas que obtienen direcciones electrónicas para enviar publicidad o cualquier otro tipo de información deben cerciorarse de que el afectado ha manifestado su consentimiento para que traten sus datos referidos a esa dirección.

El spam[32] consiste en la difusión generalizada de mensajes no solicitados a un gran número de usuarios de Internet, de forma masiva e indiscriminada. Este es susceptible de manifestarse básicamente a través de dos tipos de recursos de Internet: a) en el marco de los grupos de discusión, presentándose bajo la forma de un mensaje único enviado a varios grupos de discusión, con frecuencia sin relación con el tema que se trata o discute y complica, la tarea de los administradores que moderan o administran los temas abordados; b) por la vía del correo electrónico, que es un instrumento básico de las comunicaciones comerciales en Internet, mediante el cual se comercializa, de manera directa, bienes y servicios.

Los envíos publicitarios y/o campañas publicitarias que se realizan a través de Internet se han convertido en un medio de promoción empresarial para las empresas que ofertan por este medio sus productos y servicios[33]. Éstas tienen la posibilidad de captar miles de clientes potenciales con un costo mínimo, ya que con la conexión a Internet y la casilla de correo electrónico envían mensajes similares a miles de

[32] De acuerdo al reporte del tercer trimestre 2009 de la firma de seguridad McAfee, la lista de países generadores de spam, es encabezada por Estados Unidos (25%), y continúa: Brasil (12.1%), India (5,3%), Polonia (4,5%), República de Corea (3,1%), Venezuela (3,1%), Turquía (2,9%), Argentina (2,2%), Colombia (1,9%) y Rusia (1,8%). Entre los distintos temas que abarca el correo spam, se ubica en primer lugar, la venta de medicamentos, que alcanza un 34% del total y segundo con un 25,4%, los correos que se reciben como respuesta automática cuando una dirección de correo electrónico no existe. Ver en http://noticias.latam.msn.com/ar/ciencia_tecnologia/articulo_periodismo.aspx?cp-documentid=22548079.

[33] Un estudio de las Universidades de California, Berkeley y San Diego, en Estados Unidos, determina que con sólo un click cada 12,5 e-mails publicitarios que se envían proporciona beneficio a la empresa anunciadora. Ver en http://www.20minutos.es/noticia/428964/0/spam/rentabilidad/email/.

personas simultáneamente, evitando así el costo que similar publicidad tendría en el correo tradicional por papel, impresión y envío postal. Cuanto más grande sea el público alcanzado, mayores son las posibilidades de encontrar un consumidor interesado por el mensaje publicitario que le ha sido remitido.

Para esto, las empresas necesitan disponer previamente de una amplia base de direcciones electrónicas de clientes actuales o potenciales, o en su defecto, poder acceder a tales direcciones. Para esto, emplean distintos métodos como la recolección en forma masiva e indiscriminada de correos electrónicos en páginas web o servicios online (ya sea en grupos de noticias, foros, charlas, chat y similares), a través de cualquier tecnologías o medios; la utilización de programas de computación que permiten la inscripción de un máximo de listas de distribución a fin de recuperar las direcciones electrónicas de sus miembros o maniobras fraudulentas (concursos[34], ofrecimiento de espacios o páginas web gratuitas, etc.).

Además, en Internet se encuentra a disposición de las personas, guías y anuarios con direcciones de correo electrónico, datos de consumidores, clientes, proveedores, etc., por lo que es posible adquirir de manera legal o ilegal base de datos a sumas módicas o gratuitas. De otro lado, el empleo masivo de cookies contribuye enormemente a facilitar la posterior circulación y envío masivo de comunicaciones comerciales no solicitadas.

---

[34] La Agencia Española de Protección de Datos ha sancionado a la empresa de venta de entradas Tick Tack Ticket con 30.001 euros por el envío de correos electrónicos con fines comerciales sin consentimiento a cerca de 40.000 direcciones de correo electrónico. Obtuvo sus direcciones a través de un sorteo que invitaba a los usuarios a mandar datos de sus contactos. Ver en http://www.30minutos.es/noticia/526337/0/tick/tack/ticket/.

Uno de los ejes del comercio electrónico es la comunicación no solicitada. Aunque la práctica del "spam" es casi tan antigua como Internet, su desmesurado crecimiento y su enfoque comercial la han convertido en una amenaza para el correcto funcionamiento de la red. Esto genera conflictos, desde la perspectiva tanto de la empresa como del usuario. Desde la empresa, estas comunicaciones pueden y llegan a suponer costes suplementarios y pérdidas de productividad.

De otro lado, para el usuario, el problema se manifiesta de distintas maneras, causándole al propio tiempo, perjuicios económicos. En primer lugar, la inclusión en una lista de su dirección de correo electrónico sin su consentimiento o conocimiento; en segundo orden, la recepción de grandes cantidades de mensajes publicitarios no deseados y molestosos que lo colocan en una posición dificultosa, puesto que le puede ocurrir un posible abarrotamiento ante la recepción de múltiples mensajes no deseados, pudiendo inclusive producir la caída del sistema y no recibir aquellos mensajes que este si desea. Al ser inundadas las casillas de correo, a los usuarios les demanda mucho tiempo en clasificar.

En tercer lugar, el costo del tiempo de conexión que debe pagar el destinatario, mientras que el coste para el remitente es extremadamente bajo en comparación con los métodos tradicionales de marketing directo. En efecto, para la estimación se tienen en cuenta el costo del tiempo de conexión del usuario, por el uso de la línea telefónica, el costo de conectividad y el espacio de disco inutilizado de los

proveedores de servicios que les generan gastos indeseados[35]. Las quejas de los usuarios a los servidores ocasionan que éstos deban implementar procedimientos de filtrado.

El spam también afecta a los proveedores de acceso y a las compañías que ofrecen servicios de correo electrónico, ya que el increíble volumen de correos electrónicos que circulan día a día frecuentemente colapsa los servidores y retarda el tráfico de datos. Conjuntamente el costo de estos correos es soportado por los proveedores de servicios y proveedores de acceso en su mayor parte. Cada mensaje le cuesta dinero al primero por el uso de los servidores, de los canales de comunicación, las horas adicionales del personal, el equipo dañado, la productividad y oportunidades de negocio perdidas; costos que a su vez son en muchos casos trasladados a los usuarios. Tanto los servidores, como las compañías de correo web, trabajan en el desarrollo de herramientas que permitan identificar los correos no deseados antes de que lleguen al buzón del usuario.

Como el envío de comunicaciones comerciales no solicitadas constituye una actividad de bajo costo para las empresas electrónicas, esta situación supone un claro incentivo para que éstas utilicen esta herramienta de marketing a gran escala y hacer caso omiso de la protección de datos personales y de los problemas que ocasionan, entre los que se encuentra la afectación de la intimidad de los destinatarios, así como suponer un

[35] El correo electrónico no solicitado causa daños físicos en la propiedad personal del usuario. Cuando un correo electrónico entra en una computadora desde el servidor de correo, la información que representa queda impresa en la computadora del usuario. Al borrar ese correo, quedan agujeros en el sistema que se llama fragmentación, la cual causa daños físicos al sistema, haciendo lento al procesador. Aun cuando se haga correr el programa de desfragmentación, se causa un esfuerzo y desgaste del disco duro.

fraude a los consumidores y un ataque a la dignidad humana o a la protección de los menores. Socava la confianza de los consumidores, algo indispensable para el éxito del comercio electrónico.

La licitud de los envíos publicitarios y/o comerciales, en lo que la protección de datos se refiere, pasa necesariamente por la lealtad en la recogida y utilización de bases de direcciones de correo. El uso de las direcciones electrónicas para marketing directo está permitido exclusivamente cuando hayan sido recopiladas de manera leal y lícita, conforme a las normativas de protección de datos correspondientes.

Es preciso señalar, que si una dirección de correo electrónico es obtenida en un espacio público de Internet, su utilización para envíos comerciales electrónicos puede contravenir con el principio de finalidad ya que el internauta proporcionó la referida dirección electrónica para una finalidad muy distinta. Por otra parte, dado el desequilibrio del coste y la interrupción para el destinatario, se puede considerar que estos envíos no superarían la prueba del equilibrio de intereses, imperioso para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos.

Hay dos opciones que se le presentan a una persona para ser incorporado a una lista de distribución de correo electrónico, denominas “opt in” y “opt out”. La conocida como “opt-in”, al usuario se le informa que para ser incluido en una base de datos, deberá aceptar la opción de estar en la lista mediante la confirmación. Si éste no accede, no será implicado en la lista. Esta alternativa está basada en una prohibición

inicial de enviar comunicaciones no solicitadas, a menos que el destinatario haya previamente otorgado en forma expresa su consentimiento.

Bajo la opción "opt-in", hemos observado que la empresa formula una solicitud previa al futuro destinatario mediante la cual le pide su consentimiento para recibir comunicaciones comerciales del mismo en el futuro. Esta petición se lleva a cabo principalmente de dos maneras: primero, al momento de obtenerse una dirección de correo electrónico del usuario, por ejemplo cuando éste último ha efectuado una orden de compra en línea o cuando se registra a ciertos servicios gratuitos o pagos; segundo, mediante el envío de un correo en forma directa e individual al destinatario por el cual el anunciante le solicita su consentimiento a recibir posteriormente sus comunicaciones comerciales.

Sin embargo, ésta última forma del "opt in" tendrá frecuentemente como punto de partida una comunicación no solicitada, a saber la primera comunicación en la que el publicista solicita autorización al destinatario para enviarle anuncios en el futuro. El primer mensaje se hará gracias a la facilidad que existe hoy en día de obtener direcciones de correo electrónico directamente de los grupos de discusión, o al registro de un internauta en un sitio o de bases de datos públicas y carecerá, por lo general, del consentimiento previo del destinatario.

Por el contrario, el otro método nombrado "opt-out", al navegante se le informa que ha sido adicionado a la lista de distribución, y recibirá a partir de la próxima entrega los mensajes de la lista; en caso de que no desee la suscripción, puede cancelarla y/o oponerse expresamente desde el momento en que recibe el anuncio. Existen diferentes

maneras de organizar el sistema del opt out. La primera consiste en el establecimiento de registros que contienen la lista de las personas que se niegan a recibir todo tipo de publicidad no solicitada[36]. La otra, en una solicitud expresa del consumidor dirigida caso por caso y directamente al remitente de la comunicación o publicidad con la finalidad de que éste retire su dirección de correo electrónico de su lista de distribución o base de datos.

El "opt-out" no es el único ni el mejor sistema para proteger el derecho a la autodeterminación informativa en Internet, por lo que algunas empresas de publicidad no intrusiva optan por el procedimiento contrario "opt in", ya que es el internauta que decide suscribirse voluntariamente, según las preferencias que preselecciona y eligiendo igualmente el número de mensajes. Además no resulta suficiente y contradice las reglas de buena conducta sobre Internet que preconizan el acuerdo previo del afectado antes de la recepción de un correo electrónico comercial.

En cuanto a la regulación de este tipo de correo, existen dos posiciones a nivel internacional. Es también problemático el asunto cuando existen normativas opuestas sobre comunicaciones comerciales que den lugar a obstáculos al comercio electrónico. Muchas legislaciones, entre ellas la de los Estados Europeos, establecen la obligación de colocar una opción final en las páginas web en la cual el usuario debe

[36] Las Listas Robinson son bases de datos que almacenan los nombres y direcciones de aquellas personas que no desean recibir publicidad no solicitada. La Federación de Comercio Electrónico y Marketing directo gestiona este servicio con el fin no lucrativo y así reforzar las buenas relaciones entre los profesionales del sector y el público en general. Cualquier persona puede inscribirse en el Servicio de Lista Robinson de forma gratuita. Para ello, es necesario indicar, el medio (correo, e-mail, sms, teléfono y fax) a través del cual no desea recibir publicidad de entidades con las cuales no mantenga ni haya mantenido algún tipo de relación. Para más información https://www.listarobinson.es /default.asp

seleccionar en caso de que no desee recibir publicidad. Otros países, poseen legislaciones más estrictas, ya que invierten el sistema al establecer que los usuarios deben seleccionar la casilla adecuada para hacer una solicitud formal de que desea recibir información.

Estados Unidos ha sido el país que más ha luchado contra la utilización del correo electrónico para el envío de publicidad no solicitada. Además de las iniciativas legislativas[37] para regular la publicidad a través del correo electrónico, destacan las demandas que se han producido contra los remitentes de mensajes publicitarios no solicitados[38]. El Departamento de Comercio de Estados Unidos ha elaborado unas recomendaciones para usuarios y comerciantes sobre las disposiciones vigentes respecto de la publicidad en Internet. Se establece clara y taxativamente que las normas y usos publicitarios en el comercio general son aplicables a las mismas prácticas en el comercio electrónico

Cabe destacar que en Estados Unidos, a través de la ley Can-Spam Act of 2003, se ha establecido que todo mensaje de correo electrónico de índole comercial deberá ser

---

[37] En Estados Unidos, ya a partir del envío por propaganda por correo tradicional se generó cierta jurisprudencia "Central Hudson Gas & Electric Co. V. Public Service Communications", 447 US. 557, (1980) que limitaba este tipo de actividades por considerarlas como violatorias de la privacidad del destinatario. Con la llegada de la Internet, similares estándares fueron aplicados a la publicidad. Así, en 1996 se resolvió el caso "Cyber Promotions, Inc. v. America Online, Inc., 948 F.Supp. 436 (E.D. Pa 1996) en el cual se reconoció el derecho del proveedor a impedir el envío de propaganda no solicitada y al año siguiente una solución similar fue adoptada en "CompuServe, Inc. v. Cyber Promotions, Inc. ... 962 F. Supp. 1015 (S.D. Oh. 1997)". Luego de estos dos precedentes, en Estados Unidos se dictaron nuevos fallos, a la vez que se comenzaron a discutir posibles normativas (tanto a nivel estadual como federal). A nivel federal, el Congreso norteamericano no avanzó decididamente sobre la regulación del spam sino a partir de 2003, cuando la presión de empresas como Time Warner y Microsoft y de las legislaturas estaduales se hizo notar. La presión del sector privado se basaba en que el spam había alcanzado un nivel alarmante que afectaba económicamente a miles de corporaciones.

[38] Gigantes de la industria de Internet como America Online, Prodigy o CompuServe han demandado a empresas dedicadas a realizar campañas publicitarias a través del correo electrónico.

enviado desde una casilla "verdadera" que deberá contar con un mecanismo de baja (opt out) para el caso de que el usuario no desee recibir más comunicaciones; así como también la obligación de encabezar en los mensajes la palabra publicidad y de revelar la identidad y dirección de correo electrónico.

Tanto en la Comunidad Europea como en la Argentina[39], se establecen las condiciones de cumplimiento para las empresas del deber de información al interesado cuando los datos no hayan sido recabados directamente de ellos. Asimismo, deben informar el origen de los datos y de la identidad del responsable del tratamiento, así como los derechos que le asisten. El interesado puede oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquel, a su simple solicitud.

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), contiene exigencias para

[39] El artículo 27 (Archivos, registros o bancos de datos con fines de publicidad) de la Ley 25.326 Protección de los Datos Personales, Argentina, dispone que "1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento; 2. En los supuestos contemplados en ese artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. 3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo". Enseguida, la Dirección General de Protección de Datos Personales, a través de la disposición 4/2009 estableció que la opción para el ejercicio del derecho de retiro o bloqueo contemplada en el artículo 27 inciso tres deberá aparecer en toda comunicación que se efectúe con fines publicitarios, junto con el mecanismo previsto para su ejercicio. Por otra parte, en el año 2006, se dictó en la Argentina la primera sentencia contra el Spam, la cual se encuentra disponible en http://www.protecciondedatos.com.ar/.

los Estados Miembros que permitan las comunicaciones no solicitadas por medio de correo electrónico:

- Identificación como tales en el momento de su recepción: Garantizarán que dicha comunicación comercial facilitada por un prestador de servicios establecido en su territorio sea identificable de manera clara e inequívoca como tal en el mismo momento de su recepción, con el fin de mejorar la transparencia y facilitar el funcionamiento de los dispositivos creados por la industria.
- Consulta regular por los prestadores de servicios de las listas de exclusión voluntarias: Adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntarias en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales y las respete.
- Deberá fomentarse y facilitarse la creación por el sector competente de dispositivos de filtro; y que las comunicaciones comerciales por correo electrónico no deberán redundar en gastos suplementarios para el destinatario.

Por otra parte, el artículo 10 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia, se inclina por el sistema "opt out" al prever la exigencia del consentimiento del consumidor con carácter previo a la utilización por el proveedor de las llamadas automáticas y del fax, al tiempo que su apartado 2 contempla que el resto de las técnicas de comunicación a distancia que permitan una

comunicación individual, entre las que debe incluirse el correo electrónico, sólo pueden ser utilizadas de no existir oposición manifiesta del consumidor[40].

En ese mismo orden de ideas, en España, la ley de Servicios de la Información legitima las comunicaciones comerciales realizadas a personas con las que el prestador de servicios de la sociedad haya tenido una relación contractual previa, en la que haya procedido a recoger los datos lícitamente y utilice la comunicación comercial para publicitar o promocionar productos o servicios de su propia empresa que sean similares a los que contrató el cliente en esa relación contractual previa a la comunicación comercial. En este supuesto, se deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento con fines promocionales.

Respecto a lo anterior, la autora María Arias Pou[41] critica la ambigüedad de dicha norma ya que deja incertidumbre respecto de su aplicación, preguntándose cuándo debe entenderse que ha existido una relación contractual previa, por el concepto de productos similares, ya que es un término jurídico indeterminado que puede dar lugar a múltiples confusiones o abusos por parte del prestador de servicios.

---

[40] En adición a esto, sin embargo, la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, parece referirse a la opción "opt in" en su artículo 12, no sólo reitera la utilización de aparatos de llamada automática o fax con fines de venta directa sólo es posible con respecto a quienes hayan dado su consentimiento previo sino también que los Estados miembros no permitirán el empleo con tales fines de otros medios sin el consentimiento de los destinatarios o respecto a los destinatarios que no lo deseen.

[41] ARIAS POU. Op. Cit. p. 252.

La Asociación Española de Comercio Electrónico[42] reconoce el derecho del consumidor a oponerse siempre a las siguientes situaciones: 1. El tratamiento de sus datos, salvo que el tratamiento sea necesario para la ejecución de los contratos celebrados; 2. Que los datos sean utilizados para alguna o algunas de las finalidades determinadas en la información sobre el tratamiento; 3. A la cesión de la información a terceros.

Las empresas preocupadas por el respeto a la privacidad del cliente adoptan procedimientos sencillos, eficaces y gratuitos para que éste pueda aceptar o rechazar la recepción de mensajes comerciales electrónicos no solicitados. Del mismo modo para garantizar que no darán los datos a terceros bajo ningún concepto. Es necesario que las empresas mantengan un listado de las personas que hayan optado por no recibir información comercial.

[42] Si bien no hace referencia al correo electrónico ni a otros medios de comunicación a distancia, los artículos 30 y 31 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, son de interés en este contexto. El art. 30 limita los datos de carácter personal que pueden ser utilizados por quienes se dediquen a actividades como la publicidad o la venta a distancia, a los que figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento (apartado 4). El art. 31 establece la posibilidad de que quienes se dediquen a esas actividades obtengan de la administración una copia del llamado censo promocional, en el que figuran los datos de nombre, apellidos y domicilio del ceso electoral, con exclusión de los datos de quienes así lo hayan solicitado; remitiendo al desarrollo reglamentación la regulación de los procedimientos - que serán gratuitos - mediante los que los interesados podrán solicitar no aparecer en el censo promocional.

3.3 Movimiento internacional de datos personales en el comercio electrónico.

La interconexión a nivel mundial de las redes digitales promueve la globalización de la información, de manera que Internet constituye un medio propicio para la circulación transfronteriza de datos personales, la cual se ha convertido en un elemento importante para el desarrollo del comercio electrónico. Esto contribuye a la segmentación de las operaciones de recogida, tratamiento, cesión y cruce de informaciones en diferentes países.

El carácter global de las redes y el libre tránsito de los datos que por ellas circulan exigen una normativa también de carácter global, cuyo diseño constituye un auténtico desafío regulador, y ello fundamentalmente porque la protección de las transferencias internacionales de datos implica atenuar los derechos humanos y las libertades fundamentales con los intereses del comercio internacional. Conocer el nivel de protección de un país determinado que será destino de una transferencia de datos personales es importante para permitir el libre flujo de información a ese lugar.

Son significativos los casos de compañías multinacionales[43] que disponen de establecimientos comerciales en diversos países del mundo: cuando una empresa matriz, obtiene de una de sus sucursales en el extranjero, datos transferidos. Generalmente se trata de web cuyo diseño se ha adaptado a las singularidades

[43] Un ejemplo de esta situación, es la sanción aplicada a Microsoft Ibérica por la Agencia de Protección de Datos, originada por la utilización indebida de datos de sus clientes, desviándolos a la matriz Microsoft ubicada en los Estados Unidos.

naciones y cuya infraestructura común ha favorecido una gestión centralizada, con el consiguiente ahorro de recursos, tanto humanos como materiales.

Igualmente, un supuesto habitual es el caso consistente en prestar servicios de alojamiento de datos en un servidor, pero con la peculiaridad de que aunque el cliente esté en el que se oferte el servicio, resulta finalmente que dichos datos van a un país tercero, en relación al cual no sabe nada dicho cliente. Estos modelos de organización tienen una repercusión clara en lo relativo a la protección de los datos de los usuarios, en función de las garantías que cada país ofrece.

Por otra parte, existe el peligro de que las disparidades en las legislaciones nacionales puedan obstaculizar la libre circulación transfronteriza de datos personales; circulación que se ha incrementado en gran medida en años recientes y que van a aumentarse aún más con la introducción generalizada de nuevas tecnologías de informática y de comunicaciones. También está el temor a una deslocalización masiva de ficheros, que afectarían además a los servicios y sectores intensivos en informática y telecomunicaciones como banca, seguros, agencias de viajes y servicios médicos.

Las directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE), del 23 de septiembre de 1980, sin carácter vinculante pero si aceptada y respetada por la mayor parte de los países occidentales, marcó las primeras directrices para la protección de la intimidad en las transferencias internacionales de datos de carácter personal, tanto a nivel nacional como a nivel internacional. En ellas se abogaron por la libre transferencia, pero con las legítimas restricciones.

Las pautas para la regulación de los archivos de datos personales informatizados, adoptadas mediante resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas (ONU), de 14 de diciembre de 1990, incluyen disposiciones de control y sanciones, lo que reflejó una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos.

El criterio general es la prohibición de las transferencias -temporales o definitivas- al extranjero de datos de carácter personal que hayan sido objeto de tratamiento o recogidos para ser sometidos a tratamiento cuando el país de destino no proporcione un nivel de protección equiparable al del país remitente. Según el Grupo de Trabajo de Protección sobre Datos de la Unión Europea, creado por el artículo 29 de la Directiva 95/46/CE, es necesario que la regulación de un país contenga no únicamente unos principios de contenido y procedimientos de protección de datos personales, sino mecanismos y autoridades que efectivamente velen por la protección de dicha información.

Los normas de protección de datos personales, deben garantizar los siguientes aspectos: a) La exigencia de un tratamiento con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia; b) los datos deben ser exactos, actualizados, adecuados, pertinentes y no excesivos en relación con el objetivo para el que se transfieren o para el que se tratan posteriormente: c) Informar a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal; d) La adopción de medidas técnicas y organizativas adecuadas a los riesgos que presenta el

tratamiento por el responsable; e) Los derechos de acceso, rectificación, oposición; f) Restricciones respecto a transferencias sucesivas a otros países terceros.

En ese mismo orden de ideas, cuando se trate de categorías de datos "sensibles" se deberá establecer protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento. En el caso de que el objetivo de la transferencia de datos sea el marketing directo, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

La Comunidad Europea ha pretendido exportar sus estándares de protección en aras de proteger sus propios intereses comerciales. Ésta autoriza exclusivamente la transferencia de datos personales a países que tengan un nivel adecuado de protección de la privacidad. Con esto pretende evitar la creación de paraísos informáticos, es decir, jurisdicciones donde la carencia de leyes de protección de datos, la transforme en sitios atractivos para realizar tratamientos de datos personales que puedan ser violatorios de otras leyes de privacidad. Sin embargo, Pablo Palazzi opina que la posibilidad de encontrar estos paraísos es cada vez más alta[44].

Esto ha causado un gran problema a nivel internacional por la necesidad de evaluar si el resto de los países no europeos cumplen con los recaudos necesarios para considerar su legislación "adecuada" en términos de protección de la privacidad. Es complicada la evaluación de adecuación de regímenes legislativos de los más diversos

[44] PALAZZI. Op. Cit. p. 299.

países, cada uno con sus diversos sistemas constitucionales, legislativos, costumbres, aspectos sociales y económicos. Los sistemas legales tienen diferentes valores y diversos enfoques de regulación de datos personales.

En esa tesitura, el problema reside en encontrar cuál es el método idóneo y completo para determinar si un régimen legal determinado resulta adecuado a los estándares europeos de protección de datos personales, y aplicar ese método en forma uniforme a todas las legislaciones del mundo donde se realicen transferencia de datos personales desde Europa. Es importante esta uniformidad ya que entran en juego principios del derecho del comercio internacional que obligan a la Unión Europea a dar un trato igualitario a las transferencias internacionales de datos personales bajo las normas del Acuerdo General sobre el Comercio de Servicios (GATS).

La concreción jurídica del término nivel de protección adecuado resulta compleja e incierta. Se prevé que la decisión al respecto debe tomarse atendiendo a todas las circunstancias de la transferencia y, en particular, a la naturaleza de los datos, la finalidad y duración del tratamiento previsto, el país de origen y el país de destino final, las normas del país de destino y los informes de la Unión Europea. A este respecto, la ley española de protección de Datos, en línea con lo dispuesto en los apartados 2 a 6 del artículo 25 de la Directiva 95/46/CE, prevén mecanismos de intercambio de información respecto de la situación en terceros Estados y la posibilidad de que la Comisión Europea negocie con éstos para remediar la situación

y decidir, junto a los representantes de los Estados de si su nivel de protección es adecuado[45].

De conformidad con las normativas de protección de datos, por ejemplo en la Argentina y los países europeos, la prohibición de transferencia de datos personales de un país a otro, no regirá en los siguientes supuestos: transferencias bancarias o bursátiles, fiscales o aduaneras, conforme a su legislación específica; intercambio de datos para fines médicos; transferencias acordadas en el marco de tratados o convenios internacionales; cooperación internacional entre organismos para la lucha contra el crimen. Otras leyes poseen más excepciones tales como la formulación de reaseguros a través de contratos, grupos de empresa, etc.

En lo que concierne a la existencia de garantías apropiadas o adecuadas, el responsable del tratamiento debe ofrecer las garantías suficientes a la protección de datos personales mediante la inclusión de cláusulas contractuales apropiadas[46]. Esto presenta ciertas carencias de carácter general, en la medida en que la solución contractual no garantiza un resultado equivalente a la vigencia de legislación apropiada en el Estado de destino, lo que debe condicionar significativamente la configuración del contrato[47].

---

[45] DE MIGUEL ASENSIO, PEDRO A. (2000). *Derecho privado en Internet.* Madrid: Civitas Ediciones. p. 480.

[46] La Comisión Europea estableció, a través de la Decisión 2002/16/CE un modelo de cláusulas contractuales tipo para la transferencia de datos personales a encargados de tratamiento establecidos en terceros países. Ver en http://europa.eu.int/eur-lex/pri/es/oj/dat/2002/l_006/l_00620020110es00520062.pdf.

[47] DE MIGUEL ASENSIO. Op. Cit. p. 481.

La admisión de pactos entre las partes implicadas en la transferencia de datos es un instrumento apropiado básicamente en situaciones de intercambio estable y continuado de datos, habida cuenta del costo (de negociación y redacción) asociado a esa solución, que en particular tiende a hacerla inviable en supuestos en los que entre emisor y receptor de los datos existe una transferencia internacional aislada.

Internacionalmente se han identificado al menos cuatro modelos de sistemas de "regulación" para proteger los datos personales y el derecho a la intimidad de las personas: utilización de tecnologías, leyes generales, leyes sectoriales, autorregulación. En muchos países se recurre a una mezcla complementaria de estos modelos para garantizar un nivel mínimo de protección a los ciudadanos frente al tratamiento de sus datos personales. Otros recurren al uso de normas generales de protección de los datos personales, como los países europeos, Argentina, Canadá. En cambio, naciones como Estados Unidos usan leyes sectoriales como complemento de las normas particulares para ciertos tipos de información como la relacionada con los antecedentes penales, las historias clínicas, la información comercial y financiera.

4.1 Soluciones técnicas de protección de datos personales.

Las soluciones técnicas de protección de datos personales se agrupan bajo el título de tecnologías favorecedoras de la privacidad. Se definen como un sistema de medidas técnicas que protegen la privacidad eliminando o reduciendo los datos personales que se facilitan en la Internet, o impidiendo el tratamiento innecesario o no deseado de los mismos; todo ello sin que se pierda la funcionalidad del sistema informático en el que

operan esos datos[48]. Estas soluciones operan sobre la base de códigos de conductas con la finalidad de complementar o suplir las regulaciones territoriales cuando éstas sean insuficientes o incompletas para lidiar con la protección de datos personales más allá del marco estrictamente nacional.

Esta categoría abarca desde los anuladores de cookies, hasta los repetidores de correo (remailers) y los anonimizadores de navegación, pasando por los servidores proxy, los agentes de software y las aplicaciones criptográficas. Consiste en integrar éstas soluciones como mecanismos de protección de la privacidad, dentro de los sistemas de comercio electrónico, brindando mayores garantías. Las empresas que comercializan herramientas y programas para Internet saben que cada vez más usuarios toman conciencia del problema y están dispuestos a pagar a cambio de protección.

4.1.1 Plataforma de preferencias de privacidad.

La Plataforma de Preferencias de Privacidad funciona como una lista de preguntas y respuestas sobre el nivel de privacidad entre el navegador y el sitio web al que nos hemos conectado. En sentido amplio, puede decirse que ésta forma parte de la arquitectura y configuración técnica de Internet, permitiendo expresar a los sitios web sus prácticas de privacidad en formato estándar de modo que puedan ser leídas e interpretadas automáticamente por un agente de software que utiliza el usuario.

[48] OLIVER LALANA, DANIEL. (2003). *Estrategias de protección de datos en el comercio electrónico.* Recuperado el 02 de septiembre de 2009, de http://ciberconta.unizar.es/leccion/proteccion/descargas/pd_ecomm.pdf, p. 4.

Facilita a su vez el cumplimiento del deber de información a los consumidores que comúnmente exigen las leyes nacionales.

Por su parte, el internauta, en fin, no precisa leer las políticas de privacidad de las páginas que visita, pues lo hace el software en su lugar, comprobando si tales prácticas coinciden con las preferencias de privacidad previamente definidas por él. Se busca la forma de delegar determinados aspectos problemáticos de la interacción virtual en un protocolo destinado a negociar las protecciones de privacidad. Sin embargo, no es suficiente como garantía de protección de datos en la red.

Esto se debe a que esta instrumento no protege al internauta en los países que carecen de ese marco legislativo. La misma debe aplicarse en un contexto de normas jurídicas que sean ejecutables y deparen a todas las personas un nivel mínimo y no negociable de protección. No proporciona ninguna forma de asegurar que las compañías que la utilicen sigan sus propias políticas de privacidad ni que el sitio web que visitamos esté realmente haciendo lo que afirma hacer.

La integración técnica de ciertos principios de protección de datos se ha revelado insuficiente en este caso. Se podría sospechar que, al funcionar automáticamente, este tipo de herramientas podrían esconder información relevante desde el punto de vista de la protección del ciudadano. Se debe introducirse en la arquitectura de la red un nuevo estándar de protección de datos, no que sea el mercado quien lo incluya.

4.1.2 Agentes de software con protecciones de privacidad.

Uno de los elementos básicos del sistema de comercio electrónico son los agentes (inteligentes) de software, que son programas o aplicaciones que actúan en representación del usuario intentando alcanzar ciertos objetivos o realizando determinadas tareas sin su intervención o supervisión directa. Se conocen a los programas diseñados para acompañar al usuario en la navegación o para mejorar su comportamiento de consumo en la red. En algunos casos, se oculta en ellos alguna forma de programa espías.

Aún cuando no todos los agentes se dedican a espiar, lo cierto es que, dado su carácter de representantes y acompañantes, tienen que acumular y manejar gran volumen de información para su usuario (perfil completo), de modo que plantean siempre problemas de protección de datos y seguridad. El perfil del usuario puede extraviarse, o cederse por error. También otros agentes más potentes, actuando en representación de otros usuarios, pueden atacar a nuestro agente y robar nuestro perfil personal. El reto consiste en diseñar agentes de software que incorporen reglas de protección de privacidad y que sean capaces de eliminar o minimizar la recogida y uso de información personal.

Respecto de la herramienta analizada, la ventaja que muestra es que aspiran a implementar en sus especificaciones técnicas el modelo europeo de protección de datos personales, el cual es propuesto desde la fase de diseño de dichos agentes. Estos deben ser construidos integrando tecnologías de protección de la privacidad, estableciendo un marco de certificación para el diseño y fabricación de los agentes.

4.1.3 Infomediarios

El mercado ha concebido un tipo de proveedor virtual de servicios de privacidad, los infomediarios. Se trata de gestores o intermediarios cuya función es representar al consumidor a optimizar el valor de sus datos personales. Pese a que su funcionamiento y caracteres pueden variar según los casos, en general, el infomediario protege los datos del usuario frente a los abusos y cesiones no consentidas proporcionándole herramientas de privacidad que tratan de asegurar un determinado nivel de anonimato (correo electrónico anónimo, filtros de spam o anuladores de cookies).

Asimismo el proveedor del infomediario genera y pone a disposición del consumidor perfiles sobre los vendedores, que incluyen sus ratios de venta, el volumen de devoluciones y reclamaciones, así como el grado de satisfacción de los clientes. Al mismo tiempo, recoge y trata información completa del usuario y elabora un perfil informativo y transacciones del mismo, tanto dentro como fuera de la red. Algunos ofrecen en este sentido, la posibilidad de utilizar cookies para analizar el propio comportamiento de navegación del usuario.

La filosofía del infomediario descansa en que las empresas sólo podrán tratar los datos del perfil del usuario, disociados o no, en un ámbito de marketing consentido, el cual opera en dos direcciones: el cliente de un infomediario posee la opción de permanecer en el anonimato o de revelar su perfil a los vendedores o a las empresas de marketing directo. Cuando opte por revelar su información, el usuario recibirá siempre un beneficio determinado, como pequeños pagos en metálico, descuentos en

el precio de los productos, acceso gratuito a determinados servicios online, etc. Quien prefiera el anonimato, perderá estos beneficios pero asegurará un respeto fiel a su información personal.

Esta herramienta del mercado es positiva, en la medida en que la privacidad avanza en el mercado y es concebida incluso como una posibilidad de negocio. Pero su utilización no se encuentra exenta de riesgos. Al igual que ocurría en el caso de la Plataforma de Preferencias de Privacidad, ésta solución, con ser un buen ejemplo de utilización de las fuerzas del mercado para garantizar la privacidad, no puede desplazar el régimen jurídico de la protección de datos personales.

Dado que debe existir confianza entre el usuario y el infomediario, es preciso que existan recursos legales efectivos para el caso de que el segundo no cumpla lo que promete. Con todo, este parece ser el mejor mecanismo para compatibilizar los intereses comerciales con la privacidad del usuario. El sistema del comercio electrónico percibe las exigencias normativas de su ambiente y las reformula conforme a su propio código de funcionamiento.

4.2 Estrategias regulativas de protección de datos personales.

4.2.1 Autorregulación.

En general las normas de protección de datos significan para el sistema de comercio electrónico una imposición externa que incrementa los costes de transacción de las empresas y constituye, por ende una barrera no tarifaria para su desarrollo. Al ser

percibidas como una injerencia en el sistema, éste tiende a no cumplir las normas. Pues bien, si aceptamos que la eficacia de la legislación que pretende aplicarse a un sector de la sociedad no puede asegurarse exclusivamente a través de las sanciones, sino que depende de la colaboración de los agentes que participan en este sector, la solución a esta tendencia de incumplimiento legislativo es la autorregulación, es decir, las formas privadas de regulación.

La autorregulación supone un valor añadido respecto de la legislación general o básica, ya que la adapta a las características específicas y necesidades del sector, amplia el nivel de protección y cubre huecos legislativos, como el tratamiento de los datos de menores o la utilización de cookies. A través de ésta, pueden minimizarse los problemas de cumplimiento y aceptación de la legislación de protección de datos por parte del sistema de comercio electrónico.

Existen dos iniciativas autorreguladoras, con dos perspectivas diferentes. Una propugnada por los países más fieles a la tradición liberal, como en el caso de Estados Unidos, que promueve la autorregulación con miras a que los administradores de bancos de datos establezcan sus propios códigos de conductas o "códigos de honor" que se comprometen a cumplir frente a sus clientes y a los ciudadanos respecto de los datos personales. La otra es defendida por la Unión Europea, que ve en la iniciativa privada un complemento necesario allí donde fallan los instrumentos normativos. En España, en su ley de protección de datos de carácter personal (artículo 31) se refiere al establecimiento de "código tipo" que regulen las condiciones de organización y régimen de funcionamiento de las empresas, con respecto a la ley.

Si atendemos a los sujetos que intervienen, estos instrumentos pueden ser de dos tipos: a) las iniciativas procedentes de la comunidad empresarial y los grupos de profesionales que han intentando establecer códigos de conducta como métodos de unificación jurídica complementarios – o sustitutivos- de la iniciativa reguladora; y b) la redacción de contratos que regulen entre el particular, sujetos de los datos y las entidades transmisora y destinataria las obligaciones a las que se somete la transferencia internacional de datos. El sistema basado en políticas de privacidad es el más utilizado.

Las políticas de privacidad[49] son una manifestación de los principios de información, lealtad y finalidad en el tratamiento de datos personales. Resultan indispensables en todos los sitios Web que exijan el registro o bien ofrezcan productos o servicios y tengan formularios donde se soliciten datos personales. De igual modo, estas políticas deben integrarse en el conjunto de la organización y desarrollarse necesariamente con las de calidad, recursos humanos, estrategia, etc. Estas políticas, unidas a la seguridad informática generan valor competitivo y supondrán a corto plazo un factor clave y estratégico en la toma de decisiones de los clientes.

Internacionalmente, este mecanismo ha sido cuestionado por la falta de efectividad y cumplimiento por parte de las compañías. Autores como Casacuberta[50] han sostenido

---

[49] En la 31 Conferencia Internacional de Autoridades de Protección de datos y Privacidad, celebrada en noviembre del 2009 en la ciudad de Madrid, representantes del mundo empresarial y de la protección al consumidor coincidieron en señalar que las políticas de privacidad son un "elemento de valor añadido para las empresas" y debatieron acerca de la idoneidad de las actuales políticas de privacidad. En este sentido, señalaron la necesidad de cumplimento de unos mínimos internacionales de protección de la privacidad que puedan combinarse con la ética corporativa de las diferentes empresas. Ver en http://www.privacyconference2009.org/privacyconf2009/media/notas_prensa/common/pdfs/061109_2_global_privacidad_proteccion_datos.pdf.

[50] CASACUBERTA, DAVID. "*La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales*" en R.E.D.I. No. 10, mencionado por MONCAYO VON HASSE, ANDRÉS. (2004). El comercio electrónico:

que la autorregulación empresarial contiene insidiosas trampas, que la convierten en una técnica no funcional para regular la privacidad en la red de forma general, pasando la solución, principalmente por tres vías complementarias: la existencia de leyes protectoras de la privacidad, las tecnologías informáticas que permitan el anonimato y la toma de conciencia por parte de los ciudadanos.

También se encuentran los sellos de calidad o códigos de confianza, como por ejemplo Confianza Online, Trust-e, BBB Online, Webtrust, etc.; cuya misión es garantizar a los compradores que las empresas que los exhiben ofrecen mayores garantías en materia de autocontrol en comunicaciones comerciales, así como, mantener altos niveles de protección en lo referido a datos personales, derechos e intereses. Según un estudio sobre Comercio Electrónico[51], la percepción de estos sellos resultó ser positiva para los compradores.

4.2.2 Acuerdo de Puerto Seguro.

La protección de datos en Internet no se logra sin la participación de los Estados Unidos. En un mundo interconectado, sometido a la hegemonía de las compañías estadounidenses en la red, el derecho fundamental a la protección de datos reconocido por las legislaciones europeas sólo puede asegurarse si dichas compañías cumplen determinados estándares de protección que, además de ser onerosas para ellas, son

---

problemas y tendencias en materia de protección de la propiedad intelectual y de los datos personales desde una perspectiva argentina e internacional. *Revista Temas de derecho industrial y de la competencia,* p.312.

[51] URUEÑA, A., FERRARI, A., VALDECASA, E., BALLESTERO, M., ANTON, P., CADENAS, S., et al. (2008). *Estudio sobre comercio electrónico B2C 2008.* Madrid: red.es. Recuperado el 10 de septiembre de 2009, de http://www.aecem.org/emailing/2008/docs/B2C08.pdf. p. 15.

completamente ajenos a su cultura jurídica[52]. A través de nuevas formas de autorregulación resulta posible compatibilizar culturas jurídicas diferentes.

El modelo europeo apuntaba a ser un estándar internacional que fue obstaculizado por la oposición que presentó Estados Unidos a su aplicación extraterritorial (tanto a sucursales de ese país en la Unión Europea, como a sitios de Internet). Además la falta de un nivel adecuado de protección de datos en Estados Unidos, obligó a la Unión Europea a asegurarse que los datos allí transferidos tuvieran alguna clase de protección. Esto obligó al Departamento de Comercio de los Estados Unidos a expedir el 21 de julio de 2000 los Principios de Puerto Seguro (Safe Harbour Privacy Principles) con miras a que fuese catalogado como un país que garantiza un nivel adecuado de protección de datos personales y por ende, pudiese recibir datos personales europeos.

En materia de protección de datos, el Acuerdo de Puerto Seguro resuelve la incompatibilidad entre un sistema de disciplina legislativa y estatal de la protección de datos (Unión Europea) y otro sistema basado en la autorregulación de sectores de la economía (Estados Unidos). Mediante este pacto, se preserva la autonomía de los sistemas jurídicos nacionales o regionales, pero la compatibiliza con el orden económico mundial ya que incrementa las opciones de los usuarios y se amolda perfectamente a una estructura organizativa descentralizada y global, así como a una configuración técnica (heterogénea y abierta) de Internet[53].

---

[52] OLIVER. Op. Cit. p. 9.
[53] Ibid. p. 10.

Las jurisdicciones para vigilar la observancia por parte de las empresas estadounidenses, lo conforman el Departamento de Comercio Estadounidense y el Departamento de Transporte, en el caso del transporte aéreo. La autoridad contralor administrativa estadounidense no posee jurisdicción sobre la recogida y uso de información personal para propósito no comerciales como sería en el caso de una fundación benéfica; ni tampoco para ciertos sectores como banca, seguros, telecomunicaciones, transportes; los cuales resultan relevantes para el tratamiento de datos personales. En efecto, al margen del referido Departamento, serán otras entidades públicas con competencias similares las que vigilen la actuación de las empresas sometidas a su jurisdicción cuando la actuación de aquellas atente contra los datos personales de los particulares.

El acuerdo de Puerto Seguro implicó como mínimo una reducción del estándar propuesto por la Directiva europea 95/46/CE, ya que la autoridad contralor norteamericana, no goza de las mismas facultades con las que disponen las europeas, sus bases legales han sido cuestionadas, y al tratarse de una norma voluntaria existen cientos de sitios y empresas que no la cumplirán. Los principios de ese acuerdo constituyen una suerte de composición entre el concepto de elección y opción de las personas por el derecho norteamericano y el principio del consentimiento expreso e informado de las legislaciones europeas.

Este convenio constituye un sistema voluntario ofrecido a las entidades de Estados Unidos basado en la autocertificación y la autoevaluación, respaldado por disposiciones legales en caso de prácticas desleales o fraudulentas. Dado su carácter voluntario, la adhesión a estos principios puede derivarse bien de un programa

autorregulador propio que se adecue a los principios de Puerto Seguro, bien en la sujeción a normas estatutarias o administrativas que protejan la privacidad en forma idéntica a aquellos. La mecánica diseñada es que el Departamento de Comercio estadounidense elabora listas de empresas que se adhieren a un conjunto de reglas de protección de datos que la Unión Europea considera que ofrecen una protección apropiada.

Los exportadores de datos personales europeos que deseen comprobar si la empresa norteamericana –el destinatario de los datos- goza de la certificación de Puerto Seguro, podrán acudir al listado disponible en el Departamento de Comercio estadounidense. Las empresas que opten por permanecer al margen de estos principios podrán beneficiarse, no obstante, las excepciones permitidas en el artículo 26.1 de la Directiva europea 95/46/CE (por ejemplo, los datos transmitidos con previo consentimiento del particular) o se les exigirán garantías opcionales, como un contrato (artículo 26.2).

4.2.3 Sistema de propiedad de la privacidad y de los datos.

En Estados Unidos, la disponibilidad del derecho a la protección de datos se concibe como un elemento sujeto a la absoluta propiedad del interesado, negociable por tanto en los mismos términos que cualquier otro bien, esto es, negociar libremente con ellos. Cuando alguien posee un derecho de propiedad sobre los datos, quien desee tratarlos ha de negociar con él un precio adecuado o una contraprestación antes de poderlos obtener. Esto hace que el sistema proteja a los individuos en la medida exacta en que cada cual valore su privacidad.

Kilian[54] sostiene que resulta posible ahorrarse el creciente número de regulaciones en el sector privado si se concibe a la autodeterminación informativa como una posición análoga a la propiedad, que puede operar como tal en los procesos del mercado. Por su parte, Daniel Oliver Lalana sostiene que la naturaleza iusfundamental que el derecho de protección de datos tiene en España no impediría configurarla como una posición de propiedad, pues ésta constituye también un presupuesto de la sociedad democrática y de mercado.

En Europa, es posible vender y negociar con un derecho fundamental sin que este derecho deje de ser fundamental y sin que produzca una merma significativa en la protección del ciudadano. Puede sostenerse que el consentimiento no es ilimitado como mecanismo de legitimación del tratamiento de datos personales y que, por tanto, el sistema de protección de los datos es inaceptable en Europa. La protección de datos, en tanto que derecho fundamental, es indisponible para el individuo.

Quien defiende el sistema de propiedad equipara normativamente la protección del mercado y de la libertad de empresa con el derecho fundamental de la protección de datos. El problema es sobre qué argumentos puede sostenerse que la propiedad y el mercado deben prevalecer en el contexto actual sobre la posibilidad de control sobre los propios datos. Si las exigencias del mercado terminan imponiéndose y el sistema de propiedad transforma el sentido iusfundamental de la protección de datos en términos de valor económico, se abandona precisamente esta función, lo cual puede

[54] Ibid. p. 11.

determinar una pérdida de legitimidad del Derecho y del Estado en la sociedad de la información.

La tensión que media entre el derecho de protección de datos, el derecho de propiedad sobre los datos y la libertad empresarial reposa entre dos componentes esenciales del derecho a la protección de datos: el consentimiento y la posibilidad de control sobre los propios datos. Parte de las transacciones en línea, los consumidores son forzados a aceptar los términos contractuales impuestos por las empresas so riesgo de perder la oportunidad de negocio.

También las cláusulas de consentimiento pueden ser redactadas de formas injustas y abusivas para permitir a las compañías un tratamiento irrestricto de la información personal. Anteriormente se nos informa para conseguir el consentimiento. El problema de la articulación práctica de la prioridad del derecho de protección de datos sobre la libertad empresarial podría ser, por ejemplo, la vía de las cláusulas abusivas y del régimen de condiciones generales de la contratación.

Según Daniel Oliver Lalana, para efectuar una ponderación hay que tener en cuenta todas las circunstancias del contexto, como las carencias culturales en la materia. El ciudadano debería estar suficientemente informado y conocer las verdaderas consecuencias de las transacciones que realiza sobre sus datos, acerca del valor económico de estos y de la dimensión social y axiológica de su tratamiento. El modelo de propiedad de los datos no solo encaja perfectamente en el sistema de comercio electrónico, sino que cuadra también con el principio jurídico del consentimiento y también con las soluciones tecnológicas.

Resulta absolutamente imprescindible introducir en las empresas y organizaciones la cultura sobre protección y seguridad de datos personales. Ambas materias son aspectos claves para el desarrollo en la sociedad actual. Es necesario encontrar un nuevo equilibrio entre los intereses de la industria publicitaria, los intereses de los consumidores y la innovación.

Proteger los datos personales, al igual que la seguridad informática, genera un valor añadido tangible e intangible, y aporta ventaja competitiva en el mercado. La tecnología para proteger los datos personales de los clientes existe, es eficaz y debería garantizar la tranquilidad de los usuarios. Sin embargo, a la hora de poner en manos de terceros nuestros datos personales, debemos fijarnos en quien está al otro lado y basar nuestra decisión en la confianza y calidad de los servicios que preste la empresa en cuestión.

El carácter global de las redes y el libre tránsito de los datos exigen una normativa de protección, también global, que permita respetar los derechos humanos y las libertades fundamentales, y servir los intereses del comercio internacional. El crecimiento de la sociedad de la información, y en particular del comercio electrónico, depende -además de otros factores (como el libre acceso al los mercados, la gestión y calidad del servicio, etc.)- del nivel de protección que se otorgue a los datos en circulación.

Al momento de una empresa incursionar en el comercio electrónico, debe garantizar lo siguiente:

1. Informar al usuario sobre el tratamiento de datos personales mediante la formulación de una política de protección de datos personales en la que se especifique la finalidad de la recopilación de los datos, los posteriores utilización y divulgación de éstos, la disponibilidad de la exclusión voluntaria, los procedimientos de acceso, corrección y cancelación de los datos, los mecanismos de reclamación y enmienda, así como en su caso, una política sobre recopilación de información de menores en la que la autorización y el control de los padres sean obligatorios;
2. Las comunicaciones deben ser estrictamente confidenciales, esto es, que ningún usuario no autorizado pueda acceder a la información enviada por el cliente;
3. Deberá asegurar la integridad de la información, sin que un tercero pueda modificarla o sustraerla; que la base de datos de la empresa sea de difícil acceso así como también la utilización de una tecnología de cifrado (criptografía) para que los datos permanezcan codificados desde su envío hasta el último momento que permanezcan en esta base de datos.
4. Establecer las medidas de seguridad informática oportunas para evitar suplantaciones de personalidad en las transacciones electrónicas que se lleven a cabo de forma automática a través de la web. La autenticación del emisor y del receptor es requisito indispensable para que ambas partes puedan operar con confianza, ya que garantizan la identidades de las partes intervinientes. también la exigencia del uso de sistema de firma digital en los contratos con usuarios que deseen formalizar una relación comercial continúa.

5. Toda la información pertinente al uso de cookies en su página web, si es que las utiliza.
6. Ofrecer la opción del anonimato a los visitantes y los clientes que acceden a sus páginas.
7. Los datos personales de los menores deben ser preservados en el comercio electrónico. Las empresas, en sus páginas web, deben implementar sistemas de verificación de edad para proteger a los menores que navegan en la misma, así como asegurarse del consentimiento previo

Las organizaciones empresariales deben impartir a sus empleados capacitación continua sobre la importancia de la protección de datos. Debe exigirse a cada empleado que firme un documento en el que exprese que cumplirá con las normas de confidencialidad y seguridad que han sido establecidos por la compañía para controlar el manejo de los datos. También es preciso asegurarse de que éstos comprendan que una parte esencial de sus tareas es adoptar e implementar las normas del plan de protección de la información mantenida por la compañía.

De otro lado, las empresas deben promover y al propio tiempo, adoptar una cultura de "sensibilización en cuanto al respeto a la intimidad". Además deben actualizar y aplicar tecnologías y herramientas que perfeccionen la protección de la intimidad de sus actividades en línea, con el fin de mejorar la confianza de los consumidores.

La asunción de compromisos empresariales de autorregulación es importante. Dentro del marco legal puesto por los gobiernos, los objetivos de interés público pueden estar previstos en códigos de conductas internacionales o recíprocamente compatibles,

contratos tipo, recomendaciones, etc., que sean el resultado de un acuerdo entre la industria y otros estamentos del sector privado. La promulgación de leyes y el establecimiento de códigos éticos en protección de la privacidad/ seguridad del cliente en Internet reduce la preocupación de este y favorece el desarrollo del comercio electrónico.

Debe tenerse en cuenta que la adecuada protección de los datos personales en Internet no reposa únicamente en la existencia de una ley o regulación nacional o sectorial que proteja los datos personales y regule su recolección, almacenamiento, procesamiento o tratamiento. Una ley o regulación nacional de éstas características ha de complementarse con la implementación de sistemas de encriptación, como la firma digital tendiente a asegurar la integridad de los mensajes o comunicaciones que se realizan en Internet y la identidad de quienes las llevan a cabo.

Por otra parte, la publicación por parte de la empresa de una política justa respecto a la privacidad y seguridad en las transacciones comerciales constituye un factor que reduce el riesgo percibido por el cliente. De igual modo, el comportamiento de la empresa debe ser coherente con la política de privacidad que manifiesta, esto a los fines de evitar posible acciones civiles. Las empresas deben asociarse a sitios web de entidades independientes aseguradoras de la privacidad, puesto que reduce la preocupación del cliente y favorece el desarrollo del comercio electrónico.

Es necesario que los estados a través de mecanismos de cooperación internacional, y en diálogos de interacción permanente con la comunidad de usuarios de Internet, busquen complementar de la manera más eficiente posible las regulaciones nacionales

con autorregulaciones susceptibles de ser aplicadas más allá de la esfera estrictamente nacional sin dejar de contemplar los principios básicos que en forma coincidente pretenden proteger las leyes nacionales. También se deben reforzar los lazos de cooperación con la Unión Europea en materia de protección de datos personales.

En efecto, las leyes pueden burlarse ofreciendo datos personales desde "paraísos informáticos", países donde la ley nada dice acerca de tales conductas, tarea nada complicada dada la existencia de las tecnologías y redes mencionadas (Ej. Internet). Este problema sólo podrá ser resuelto mediante la armonización internacional de leyes. En la medida en que todas las leyes no establezcan los mismos criterios rectores, surgirán los ya mencionados paraísos informáticos, fácilmente accesibles desde cualquier lugar del mundo, desde los cuales se podrán comercializar datos personales sin recibir sanción alguna. El dictado de leyes similares, que contemplen los mismos derechos y deberes, es la única salida viable que se nos presenta.

SECCION DE REFERENCIAS

BIBLIOGRAFIA

Doctrina:

ARIAS POU, MARÍA. (2006). *Manual Práctico de Comercio Electrónico.* Madrid: La Ley.

BARRIUSO RUIZ, CARLOS. (1998). *La contratación electrónica.* Madrid: Editorial Dykinson.

DE MIGUEL ASENSIO, PEDRO A. (2000). *Derecho privado en Internet.* Madrid: Civitas Ediciones.

DRUMMOND, VÍCTOR. (2004). *Internet, privacidad y datos personales.* (Trad. Isabel Espin Alba). Madrid: Editorial Reus.

CORRIPIO GIL-DELGADO, MARÍA DE LOS REYES. (2000). *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet.* Madrid: Agencia de Protección de Datos.

FERNÁNDEZ DELPECH, HORACIO. (2001). *Internet: Su problemática jurídica.* Buenos Aires: Abeledo Perrot.

PALAZZI, PABLO A. (2003). Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. En *Derecho de Internet y Telecomunicaciones* (p. 293-355). Bogotá: Legis Editores.

REMOLINA ANGARITA, NELSON. (2003). Centrales de Información, habeas data y protección de datos personales: avances, retos y elementos para su regulación. En *Derecho de Internet y Telecomunicaciones* (p.357-435). Bogotá: Legis Editores.

RIBAS ALEJANDRO, JAVIER. (1999). *Aspectos jurídicos del comercio electrónico en Internet.* Pamplona: Editorial Aranzandi.

RODRÍGUEZ HAUSCHULD, VICTORIA. (2007). *Derecho informático.* Buenos Aires: Editorial Aplicación Tributaria.

SARRA, ANDREA VIVIANA. (2001). *Comercio electrónico y derecho,* (2ª ed.). Buenos Aires: Editorial Astrea.

Artículos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2000). *Recomendaciones al sector del Comercio electrónico, para la adecuación de su funcionamiento a la ley orgánica 15/1999, de 13 de diciembre de 2000, de protección de Datos de Carácter Personal.* Recuperado el 01 de septiembre de 2009, de https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/index-idesidphp.php#0103.

ANCOS FRANCO, HELENA. (2000). *La progresiva configuración de las transferencias de datos como objeto del trafico comercial internacional.* Recuperado el 02 de

septiembre de 2009, de http://www.revistasice.com/cmsrevistasICE/pdfs/ICE_78 8_147-160__00A20AB61C85EDC3D4FE201287AE8E22.pdf

CASTAÑEDA GARCÍA, JOSÉ A. & MONTORO RÍOS, FRANCISCO J. (2005). *La preocupación por la privacidad/seguridad como barrera al desarrollo del comercio electrónico.* Recuperado el 02 de septiembre de 2009 de http://www.revistasice.com/cmsrevistasICE/pdfs/PICE_2835_25-40__38BAF95B8EC0CD6C2481B096512DDAEA.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTICULO 29, (2000, febrero), *Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico*. Recuperado el 01 de septiembre de 2009, de https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2000/common/pdfs/Dictamen-1-2000-sobre-determinados-aspectos-deprotecci-oo-n-de-datos-en-el-comercio-electr-oo-nico.pdf

MONCAYO VON HASSE, ANDRÉS. (2004). El comercio electrónico: problemas y tendencias en materia de protección de la propiedad intelectual y de los datos personales desde una perspectiva argentina e internacional, *Revista Temas de derecho industrial y de la competencia*, 6, 275-345.

OLIVER LALANA, DANIEL. (2002). *Código invisible y pequeño gran hermano.* En II Congreso Mundial de Derecho Informático. Madrid. Recuperado el 02 de septiembre de 2009, de http://www.ieid.org/congreso/ponencia.htm

OLIVER LALANA, DANIEL. (2003). *Estrategias de protección de datos en el comercio electrónico.* Recuperado el 02 de septiembre de 2009, de http://ciberconta.unizar.es/leccion/protección/descargas/pd_ecomm.pdf

OLIVER LALANA, DANIEL. (2003). *Legislación de protección de datos y comercio electrónico.* Recuperado el 02 de septiembre de 2009, de http://ciberconta.unizar.es/LECCION/protección/

RUIZ MIGUEL, CARLOS. (s.f). *Protección de datos y comercio electrónico,* Recuperado el 02 de septiembre de 2009, en http://web.usc.es/~ruizmi/pdf/e~com.pdf

URUEÑA, A., FERRARI, A., VALDECASA, E., BALLESTERO, M., ANTON, P., CADENAS, S., et al. (2008). *Estudio sobre comercio electrónico B2C 2008.* Madrid: red.es. Recuperado el 10 de septiembre de 2009, de http://www.aecem.org/emailing/2008/docs/B2C08.pdf.

Normativas:

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, España.

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

Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia.

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior.

Ley 25.326 de Protección de los Datos Personales, Argentina.

Páginas web:

http://www.proyectopyme.info/venta-datos-personales-mayor-fuente-ingresos-portales/2-13-8-13.htm.

http://www.elpais.com/articulo/tecnologia/Grupos/internautas/reclaman/Congreso/EE/UU/medidas/proteger/privacidad/elpeputec/20090902elpeputec_2/Tes

http://noticias.latam.msn.com/ar/ciencia_tecnologia/articulo_periodismo.aspx?cp-documentid=22548079.

http://www.30minutos.es/ noticia/526337/0/tick/tack/ticket/.

http://www.privacyconference2009.org

https://www.agpd.es

https://www.protecciondedatos.com.ar/

https://www.privacyalliance.org/

https://www.aecem.org/

https://www.confianzaonline.es/

https://www.ftc.gov/privacy/

https://www.datospersonales.org/

https://www.listarobinson.es/default.asp

CURRICULUM VITAE

Calle 4 C No. 1 Mirador Norte,

Distrito Nacional, República Dominicana

Teléfonos: 809 482-8092; 809 599-3260

Emails: ariellapepen@hotmail.com; ariellapepen@yahoo.es

Áreas de Interés

Legales

Management General

Academia/ Investigación

Formación Académica

2008-2009 *Maestría en Derecho y Dirección de Empresas.*

Universidad de Palermo. Buenos Aires, Argentina.

2003-2007 *Licenciada en Derecho.*

Pontificia Universidad Católica Madre y Maestra.

Experiencia Profesional

- ***Estudio Jurídico Dr. Arrechea.*** *Buenos Aires, Argentina:* Junio 2008– Diciembre 2009

Asistir al equipo de profesionales que laboran en dicho estudio. Tareas administrativas en general del estudio. Manejo y trámites de procesos. Redacción y confección de escritos y demandas. Organización del estudio.

- ***Suprema Corte de Justicia***. *Séptimo Juzgado de la Instrucción del Distrito Nacional y Primer Juzgado de la Instrucción del Distrito Nacional, República Dominicana: 2004– Marzo 2008*

Análisis y estudiar expedientes penales remitidos a mi consideración. Verificar que los expedientes cumplan con los requerimientos establecidos en cada caso. Elaboración, redacción y motivación jurídica de modelos de sentencias, autos, resoluciones. Asistencia al juez y al secretario en sus labores. Ofrecer ayuda, información que requieran los usuarios de los expedientes. Localizar, archivar expedientes, documentos. Mantener actualizado el registro y archivo de leyes, decretos, libros jurídicos y documentos relacionados con la jurisdicción de la Instrucción. Preparar informes sobre las investigaciones jurídicas. Estudiar leyes y códigos que sirvan de apoyo en el análisis de los expedientes.

- *Intercambio cultural "Summer Work and Travel 2007" auspiciado por la Oficina Dominicana de Turismo Educativo en Mackinac Island, Michigan, Estados Unidos en la empresa The Island House & Rena's Fudge Shops:* Mayo 2007 – Septiembre 2007

Producción, venta, atención al cliente, facturación de dulces artesanales.

Idiomas

1998 -2002 *Instituto de Idiomas FISK. Inglés. Nivel Avanzado*.

2002-2004 *Alianza Francesa de Santo Domingo. Francés. Nivel Intermedio.*

Conocimientos Informáticos

Windows, Word, Excel, Power Point, Access, Outlook, Publisher, Internet.

Otros Cursos y Seminarios

Inducción al Servicio Judicial: *Suprema Corte de Justicia*

Diplomado en Derecho Procesal Penal: *Fundación de Jóvenes para el Progreso*

Conociendo el Mercado de Valores: *Escuela Bursátil Superintendencia de Valores*

Diplomado en Derecho Inmobiliario: *Fundación Democracia y Derechos Humanos*

Diplomado en Derecho Laboral: *Fundación Democracia y Derechos Humanos*