

TRÁFICO DE DATOS PERSONALES: SU AFECTACIÓN A LOS DERECHOS PERSONALISIMOS*

Eliana Mariel Ferrero¹

Anabella Schutz²

RESUMEN

Los **“Datos Personales”** se han convertido en un **“activo más”** que cotiza a un alto valor en el mercado, cuya transmisión y comercialización opera preferentemente a través de Internet, dando origen a un incipiente y acaudalado negocio en torno a ellos: **“El Tráfico de Datos Personales”**.

Como consecuencia, el ámbito de privacidad de las personas es cada día más reducido, generando así la imperiosa necesidad de proteger los datos personales y el deber como sociedad de luchar por la salvaguarda de la intimidad ante la inminencia de un *“floreciente mercado”* que por el vasto caudal de dinero que genera no parece ser una *“moda pasajera”* sino un negocio que llegó para quedarse.

Tráfico de Datos Personales

En la actualidad, estamos inmersos en lo que podría individualizarse como la **“Revolución Tecnológica de la Información” (RTI)**, iniciada aproximadamente hace tres décadas y cuya nota distintiva consiste en haber alterado los dos parámetros básicos en que se desarrolla la actividad humana: el espacio y el tiempo. A la vez, que ha introducido cambios radicales en diversos aspectos de la vida tales como: las relaciones humanas, el trabajo, el comercio, la industria; ha simplificado la comunicación e interacción, el conocimiento y sobre todo se ha masificado el acceso y manejo de la *“información”*.

Indudablemente, el motor que ha dado forma a estas mutaciones es lo que se conoce como **“Tecnologías de la Información y la Comunicación” (TICs)**, las cuales se conciben como la consumación del encuentro de dos subconjuntos, uno, representado por las tradicionales ‘Tecnologías de la Comunicación’ (TC) -constituidas, principalmente, por la radio, la televisión y la telefonía convencional- y otro, encarnado por las ‘Tecnologías de la Información’ (TI) -

*El presente trabajo es una síntesis del Seminario sobre Aportaciones Teóricas y Técnicas Recientes del mismo título, cuyo texto puede ser consultado en la Biblioteca Central de la Universidad Nacional de La Pampa.

¹ Estudiante de la carrera de Abogacía de la Universidad Nacional de La Pampa; mail: elianaferrero@hotmail.com.

² Estudiante de la carrera de Abogacía de la Universidad Nacional de La Pampa; mail: ana-schutz@hotmail.com.

caracterizadas por la digitalización de las técnicas de registro de contenidos (informáticas, de comunicación, telemáticas y de interfaces) (Sal Paz, 2010).

Por su parte, el estadio actual de desarrollo de la civilización humana ha sido denominado **“Sociedad de la Información”**, que es aquella en la que la información se presenta como un elemento clave de poder y como factor preponderante del desarrollo de las sociedades. La información se ve sometida a las reglas del mercado, de la oferta y la demanda, además de consumirse, almacenarse o procesarse.

En la mentada sociedad, **Internet**, la Red de Redes que conecta computadoras a escala mundial, es el estandarte del cambio técnico de los últimos años. Aquella podría definirse como **“Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación”**³, ha producido un cambio sustancial en la forma de transmitir la información.

La cantidad de información que circula en la Red es de dimensiones inimaginables, resultando alarmante que una buena parte de esa información esté constituida por **“Datos de carácter Personal”**, los cuales son utilizados y comercializados con diversidad de propósitos, sin solicitar el consentimiento de su titular (recaudo básico de licitud).

En efecto, el **tratamiento de datos personales** se ha convertido en una práctica habitual en nuestros días y su comercialización en un negocio que mueve un inmenso caudal de dinero. De allí, que cada vez más personas, tanto de existencia física como ideal, se han abocado a la recolección, entrecruzamiento y transmisión de información confidencial.

El caldo de cultivo de este floreciente negocio ha sido la presencia de una creciente demanda, es decir, personas, empresas, organizaciones, etcétera, dispuestos a desembolsar el dinero que sea necesario para obtener dicha información, sumado a una innumerable variedad de tecnologías que han sido colocadas a su servicio.

La consecuencia directa e inmediata radica en la constante afectación de los derechos de las personas involucradas, quienes son sin duda las víctimas del **“Tráfico de Datos Personales”** que constituye un fenómeno actual cuyas múltiples implicancias analizaremos a continuación.

La Ley 25.326 de **“Protección de Datos Personales y Habeas Data”** en su artículo 2 define a los **“Datos Personales”** como: **“Información de cualquier tipo referida a personas físicas o de**

³ Diccionario de la Real Academia Española, vigésima segunda edición.

existencia ideal determinadas o determinables”. “Son una subespecie de los datos en general” (Peyrano, 2002).

Los datos personales son aquellos que nos identifican como individuos, o que al combinarlos permiten nuestra identificación y que pueden servir para confeccionar nuestro perfil ideológico, racial, sexual, económico o de cualquier otra índole. Se consideran tales: nombre y apellidos, fecha de nacimiento; número de teléfono, dirección postal y electrónica; datos sanitarios (enfermedades, abortos, cirugía estética, etc); orientación sexual; ideología, creencias religiosas, afiliación sindical, estado civil; datos económicos: bancarios, solvencia, compras; consumos (agua, gas, electricidad, teléfono); datos judiciales (antecedentes penales); datos de navegación en la web, etc. Los datos personales podría decirse que son de propiedad de cada individuo. Con ello queremos denotar que nos pertenecen y gozamos del derecho a la protección de nuestros datos, el cual no se encuentra consagrado constitucionalmente en forma autónoma.

Asimismo, la mentada ley consagra a los “*Datos Sensibles*” como categoría dentro de los datos personales y los caracteriza como “aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”. En particular, tales datos son los que toda persona desea salvaguardar de la injerencia de terceros, dada su estrecha e indisoluble vinculación con su esfera privada, motivo por el cual merecen ser protegidos con mayor intensidad.

Su vinculación con el ámbito privado de los individuos

Hasta hace unos años, las fronteras del ámbito privado estaban bien definidas y coincidían en general con la esfera del propio hogar, reservado a la familia. El tiempo, la distancia, los escasos y costosos medios de transporte y de comunicación permitían salvaguardar la privacidad con bastante facilidad.

Con el advenimiento de las TICs los impedimentos de tiempo y distancia desaparecieron por completo, favoreciendo la conformación de una gran aldea global en la que comunicarse y obtener información de otras personas son operaciones que llevan sólo unos segundos. En pocos años hemos sido testigos de un cambio radical en las comunicaciones que parece no tener vuelta atrás... Después de todo ¿quién querría volver a comunicarse por carta, no?

Si bien es cierto que las TICs han traído consigo evidentes **ventajas** en el acceso a la información, al permitir un acceso rápido y eficaz desde cualquier parte del planeta, el envío a

distancia de la misma y su almacenamiento masivo, sumado a su instantaneidad, interactividad, ubicuidad, e interacción en tiempo real y diferida; permitiendo trasladar la globalidad al mundo de la comunicación. No obstante, no podemos quedarnos solo con su lado positivo siendo que *“no todo lo que rodea Internet son luces, ya que también se localizan sombras todavía sin disipar”* (Fernández Rodríguez, 2004: pág 10).

Los Datos Personales como “mercancía”

En una sociedad globalizada en donde impera la “Ley del Mercado”, con valores como el “consumismo”, manejar los datos sobre los gustos, preferencias, hábitos de consumo, posibilidades económicas, nivel de educación, la salud y las costumbres de miles de personas puede resultar un buen negocio, dado que ello les permitirá a las empresas fabricantes de productos orientar su producción y optimizar el uso de sus recursos en producir aquello que más ventas les garantice.

Además, existen otros actores sociales que utilizan nuestros datos, con múltiples fines:

✓ *El marketing directo*: existen empresas de marketing que se dedican a elaborar publicidad a medida de los clientes, de acuerdo a sus gustos e intereses, logrando con ello mayor eficacia. Es habitual que nos llegue a nuestro correo electrónico ofrecimientos de todo tipo, aunque vinculado a nuestras necesidades de consumo del momento.

✓ *Elaboración de estadísticas y control*: También el Estado puede tener interés en recabar nuestros datos, en principio, con fines de control por ejemplo respecto de la propagación de alguna enfermedad como la Hepatitis B que le permita evaluar la necesidad o no de campañas sanitarias de vacunación y prevención. Sin embargo, el hecho de que el Estado y sus agentes dispongan de demasiada información personal de la población puede implicar un grave riesgo, sobre todo cuando se producen quiebres institucionales. Hay muchos ejemplos en la historia que evidencian que cuando los gobiernos devienen totalitarios los datos personales fueron utilizados con fines persecutorios y discriminatorios.

✓ *Exclusión de cobertura médica*: Las empresas de prepagas suelen recurrir a los rastros de navegación de los usuarios en la web a fin de chequear el posible padecimiento de alguna enfermedad en sus clientes que pudiera ocasionarle grandes erogaciones, por ejemplo: sida, cáncer o tal vez el consumo de alguna droga o medicamentos costosos. O bien suelen recurrir a

bases de datos para conocer datos genéticos y a partir de allí evaluar el riesgo que cada cliente le ocasiona.

✓ *Exclusión de asegurados*: Iguales limitaciones se aplican a los asegurados que quedan fuera del sistema de seguros, ya sea de vida, de retiro, o la cobertura de siniestro de otra índole, etcétera.

✓ *Determinación del perfil de futuros empleados*: “En oportunidades se han formado bases de datos de personas que no pueden acceder a un trabajo. Durante el 2001, en Argentina, se intentó formar una base de datos de los empleados que habían iniciado demanda contra sus empleadores. Una rápida reacción del Ministerio de Trabajo lo impidió” (Uicich, 2009, pág 81).

✓ *Fines delictivos*: Las organizaciones criminales suelen hacer un estudio de sus posibles víctimas antes de actuar, por ello nuestros datos pueden serle de gran utilidad, por ejemplo: a la hora de planear un secuestro resulta vital que la familia del secuestrado disponga de los fondos que se les pretende requerir.

✓ *Informes de solvencia*: A las empresas de crédito les interesa conocer la solvencia real de sus clientes antes de proporcionarles cualquier tipo de préstamo.

✓ *Otros destinos* que quedan librados al arbitrio de la ilimitada imaginación humana, para satisfacer infinidad de “caprichos”: popularidad, rédito económico, social, sexual, etc.

De lo expuesto, podemos afirmar con total convicción que los Datos Personales se han convertido en una “**mercancía**” que cotiza a un alto valor en el mercado, generando la aparición de un “**florecente negocio**”, junto con la proliferación de redes criminales que se dedican a su tráfico.

La “captura” de Datos Personales

El dato personal puede ser y en la práctica es manipulado. Cada día es más frecuente que nos soliciten que completemos nuestros datos, en muchos casos, con la excusa de brindarnos un mejor servicio, más personalizado y acorde a nuestros intereses particulares. También es habitual que en los comercios que efectuamos compras se realicen sorteos de espectaculares premios, siendo requisito indispensable para participar de ellos completar un cupón con nuestros datos. En ocasiones, también incluyen encuestas sobre nuestras preferencias de consumo. Lo mismo ocurre a nivel virtual, a cada paso que damos se nos solicita registrarnos.

En principio, podría decirse que efectivamente se nos brindan servicios y publicidades cada vez más acordes a nuestros gustos e intereses, lo cual puede resultar cómodo y ventajoso.

Sin embargo, lo cierto es que en la mayoría de los casos los fines para los que se recaban nuestros datos personales no son tan inocentes y a nuestro beneficio como nos dicen. En efecto, si se nos dijera el verdadero destino de ellos, con seguridad nos negaríamos a brindarlos.

Nos referimos a que las empresas recaban nuestros datos y sin requerir consentimiento alguno, los utilizan en beneficio propio directo o bien los venden a terceras personas o empresas. Es por ello, que cuando nos invaden el correo electrónico con publicidades no entendemos bien de dónde han conseguido nuestra dirección.

Hasta aquí, hemos relatado el caso en que nosotros mismos brindamos nuestros datos y ellos son utilizados con un destino diverso al que se nos había indicado. No obstante, existe aún una metodología aún más invasiva para nuestra privacidad que consiste en la utilización de modernas tecnologías para averiguar los hábitos, gustos y costumbres de los navegantes de la web, sin que logremos siquiera advertirlo.

En tal sentido, debemos mencionar a las *cookies* (galletitas en lengua inglesa) como una forma de apropiación de información muy eficaz, las cuales consisten en archivos de texto que algunos servidores piden a nuestro navegador que grabe en el disco duro de nuestra computadora, con información acerca de lo que hemos estado haciendo por sus páginas. Se trata de ficheros que recaban datos de navegación, sin que el usuario detecte que está siendo inspeccionado.

“Las *cookies* no fueron creadas con la intención de violar la intimidad. Su origen fue en 1995 de la mano de Netscape para que la versión 2.0 de su navegador pueda brindar una versión más personal y conveniente” (Uicich, 2009, pág 82). Una de sus utilidades es la personalizar las páginas más visitadas, lo que permite al usuario acceder a la sección que le interesa descartando otras, o que se cargue la página en el idioma elegido inicialmente, o que la carga sea más rápida en la sección que presenta mayor interés.

Pero también, estas *cookies* permiten el estudio minucioso sobre los hábitos de consumo del internauta. Si éste no adopta ninguna medida de bloqueo las *cookies* se irán almacenando en el directorio de su disco duro y facilitarán la formación del perfil del navegante. Al saber sus preferencias en la web se conocen las preferencias en la vida.

En este orden de ideas, lo esencial es el respeto de la voluntad del usuario, ya que debe ser éste quien preste su **consentimiento** para dar a conocer sus datos personales, el cual debe reunir

ciertas características: ser libre, expreso e informado. Las empresas web que las utilizan deberían brindarle la totalidad de la información necesaria, pertinente y suficiente para poder decidir si acepta o no a la *cookie*. Por defecto, el navegador permite las *cookies* y no avisa de su recepción, así como los sitios no avisan de su envío: esto es una inversión de la carga. El consentimiento no puede presumirse: obtenido de esta manera no reúne los requisitos anteriormente mencionados.

“Cuando los datos que aporta la *cookie* son identificables con una persona determinada o determinable que no ha prestado su consentimiento para el posterior tratamiento de ellos, debe considerarse que el dato se obtuvo en forma **ilegal** siendo responsable la empresa por su manejo y por la utilización indebida de los datos personales” (Uicich, 2009, pág 85).

Por otro lado, las descargas de archivos también pueden entrañar riesgos, ya que con esa operación puede instalarse en el equipo un *software malicioso* con diferentes finalidades: borrado de datos, robo de contraseñas y datos personales, seguimientos de los sitios webs visitados, etcétera.

Al mismo tiempo, la evolución de las tecnologías hace que cada día surjan nuevas formas de captar nuestros datos sin que logremos advertirlo. Así por ejemplo es frecuente que capten nuestra imagen y comportamiento con *cámaras de videovigilancia* y nuestra voz cuando llamamos a *servicios de atención al cliente*; o somos fotografiados por *cámaras digitales* de cualquier particular que podrían terminar en la web, revelando datos o actividades de nuestra vida cotidiana que nosotros mismos no publicaríamos.

Otra práctica no menos frecuente consiste en captar y almacenar nuestros datos cuando pagamos con *tarjetas de crédito o débito*, lo que permite conocer quienes somos, las transacciones que efectuamos, los comercios en lo que compramos, la ciudad en la que se concretaron las operaciones. Una vez más, si relacionamos esos datos es posible deducir nuestros gustos, hábitos, preferencias de consumo, forma de vida, nivel socio-económico, etcétera.

Como se puede observar, las modernas y eficientes tecnologías de distinta índole, incluso aquellas que no han sido diseñadas con ese objetivo, facilitan la circulación de un caudal de información personal de cantidades ilimitadas que es explotada con fines comerciales. El ciudadano común está lejos de llegar siquiera a imaginar el valor que tienen sus datos, la multiplicidad de modos en que son manipulados, ni tampoco quienes tienen acceso a los mismos y con qué fines o intenciones.

Afectación de los Derechos a la Intimidad, al Honor y a la Imagen Personal

Los derechos a la intimidad, al honor y a la imagen personal están siendo vulnerados mediante la utilización de Internet.

La realidad se agrava si tomamos en cuenta que es imposible restablecer los derechos anteriormente mencionados, una vez que han sido atropellados. Veamos la pluralidad de situaciones y actores que atentan contra los mismos.

- **Afectación por las Empresas:** En los últimos tiempos, se han dado a conocer hechos que evidencian el cambio de las tendencias de seguridad en Internet, viéndose afectado el derecho a la intimidad de las personas por parte del sector empresarial, que recurre a determinadas estrategias para formar bases de datos con información de sus clientes.

La irrupción de las TICs facilitó la captación masiva de datos que son almacenados en **bases de datos electrónicas**: ficheros de capacidad y posibilidades de interrelación ilimitadas, construidas a partir de los rastros de navegación y la subsiguiente elaboración de perfiles de usuarios.

Dichas bases de datos permiten el manejo de grandes volúmenes de información a bajo costo y con una velocidad en su búsqueda que las convierte en una forma muy efectiva para inmiscuirse en la vida privada de terceros. Podemos citar como ejemplo a Mastercard On line: una base de datos de 1,2 terabytes de información sobre transacciones con tarjetas de crédito, que esta empresa pone a disposición de las 22.000 compañías que constituyen su clientela.

Las empresas de publicidad y de marketing directo cruzan, en muchas ocasiones, sus bases de datos personales, obteniendo con ello, nuevos datos incluso de carácter sensible. Tales datos personales no sólo son acumulados y registrados, sino que también se procede a su transferencia, que puede derivar en intercambio de datos o bien su venta a terceras personas o empresas, sin autorización de los afectados.

Lo que resulta verdaderamente alarmante es la existencia de un **mercado de datos personales**. Existen empresas que se dedican exclusivamente a su venta a través de Internet, las cuales otorgan información de las personas como un servicio a cambio de un pago en dinero. Brindan datos tales como nombre y apellido, DNI, fecha de nacimiento, estado civil, domicilio, teléfonos, nombre del cónyuge e hijos, profesión, número de CUIT y CUIL, número de ingresos brutos, situación frente a la AFIP, empleados en relación de dependencia, historia laboral, juicios como actor y como demandado, cheques rechazados, sociedades, propiedades, datos bancarios, datos del sistema de salud, entre otros datos.

El problema es que la Ley de Protección de Datos Personales no es muy clara en este sentido y, en parte, es ese vacío legal lo que permite que las empresas puedan lucrar con los datos personales, rozando el límite con lo ilegal.

Es evidente que la garantía constitucional argentina de la protección de la intimidad está sumida en una profunda crisis. “Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, ya no están sólo reservadas a Dios. Están también reservadas a Microsoft, a Oracle, a Mastercard, a American Express, a Telefónica, etc. Están reservadas a ese nuevo olimpo de dioses paganos que intervienen, escudriñan y censan nuestras vidas sin pedirnos permiso” (Giuliano, 2000, pág 7).

- **Afectación por el Estado:** La conservación de datos por parte de los Estados es una medida necesaria, siendo posible siempre que la misma cumpla con el respeto a los derechos humanos y libertades fundamentales de todos, y en particular, de las personas afectadas.

“Lo ideal es que dichos datos sean conservados por un determinado período de tiempo, y que los mismos sean utilizados para fines específicos de orden público, como la protección y defensa de la seguridad nacional. Se debe garantizar que éstos estén disponibles con fines de prevención, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada” (Uicich, 2007).

No se debe perder de vista que los derechos a la intimidad de las personas y la protección de datos están contemplados en la Constitución Argentina y en Tratados Internacionales. Es por esta razón que el Estado debe restringir las posibilidades de compartir datos sensibles y limitar la recolección, el procesamiento y la retención de información personal al cumplimiento de objetivos específicos, sin que esto constituya una medida intrusiva que sitúe a la tecnología al servicio del control social.

- **Afectación a través de las Redes Sociales:** De todas las mutaciones que trajo consigo la masificación del uso de Internet, la más relevante quizás para el ciudadano común tiene que ver con las **Redes Sociales**. Este fenómeno nuevo ha afectado a la forma en la que nos relacionamos y el desarrollo de la personalidad. “Tal es así que toda persona ahora tiene al menos dos personalidades e identidades: la real y la digital” (Cao Avellaneda, 2012).

Las llamadas redes sociales online consisten en servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e

información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado (Gonzalez Frea, s/f).

Ahora bien, si nos detenemos a pensar en la cantidad de información que lanzamos a diario en la Red, la cuestión resulta en verdad preocupante dado que no existe conciencia de que los datos personales subidos a la web pueden tener destinos diversos. Es claro que las redes sociales potencian ciertos peligros en torno a nuestros datos personales: no debe sorprendernos que cada red social tenga a su disposición una mega base de datos digitalizados que puede comercializar con sus anunciantes y demás empresas. También es frecuente la utilización de fotografías en la publicidad de servicios, productos y marcas, sin el consentimiento de la persona.

Asimismo, existen terceros que se valen de las redes sociales para perpetrar hechos ilícitos, siendo los menores los más propensos a ser víctimas debido a la confianza y facilidad con que brindan información personal. De allí que han ido apareciendo nuevas figuras delictivas tales como: el *grooming* (utilización de medios informáticos para tomar contacto con un menor de edad, creando un ámbito de confianza, con el objeto de concretar alguna acción de pedofilia); el *ciberbullyng* (se define como acoso entre iguales en el entorno de las TICs, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños); la *usurpación de identidad* (creación de perfiles falsos en redes sociales para ejecutar acciones de defraudación bancaria o pedofilia), etcétera.

Una peculiar característica en el uso de las Redes Sociales que las distingue de forma tajante respecto de otros modos de recolección y apropiación de datos personales es que son los mismos usuarios quienes exponen “voluntariamente” su vida privada o la de terceros ante los ojos de millones de personas. Así, cuando un usuario de la Red Social efectúa una publicación puede afectar:

.- **Privacidad personal:** los efectos sobre su privacidad pueden tener un alcance mayor al que consideran en un primer momento.

.- **Privacidad de terceros:** es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información de terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata (Gonzalez Frea, s/f). A su vez, la persona afectada puede iniciar una acción judicial para reclamar los daños y perjuicios que la publicación le hubiera ocasionado. La entidad de la reparación estará dada por la magnitud del daño causado, en cada caso.

En este orden de ideas, se ha expresado que “los usuarios exponen su **intimidad** a diario, con efecto compulsivo, mediante la divulgación y posteo de cualquier tipo de dato personal que va desde un pensamiento u opinión hasta una foto familiar, pasando por el fragmento de una canción hasta un video erótico” (Tomeo, 2012). “La influencia es evidente y el fenómeno es actual. Para una persona una foto incómoda o un comentario desafortunado puede impactar en su vida personal hasta perder su trabajo, su matrimonio y sus posibilidades de progreso. La red no perdona y una vez que un contenido se "subió" es muy difícil de bloquear o eliminar” (Tomeo, 2012).

En efecto, otro de los derechos más quebrantados a través de la web es el **Derecho a la propia Imagen** que consiste en el poder que tiene cada persona de captar, reproducir y publicar su propia imagen cómo, dónde y cuándo desee, y a su vez, la posibilidad de brindar su consentimiento o no para que la misma sea divulgada por terceros.

Ya hace tiempo que encontramos violaciones al derecho a la imagen, acorde con las tecnologías vigentes en cada época. Basta recordar el emblemático caso "*Ponzetti de Balbín*": la transgresión al derecho a la intimidad y a la imagen venía determinada por la publicación en una revista de una fotografía capturada por un fotógrafo⁴. En cambio, en la actualidad es común que sean las mismas personas afectadas las que toman sus fotografías o filman videos íntimos, los cuales son subidos a la red por desconocidos. Ahora es Internet el medio utilizado para propiciar el daño e infringir los derechos.

Como vemos, cambian los sujetos que captan las imágenes y los medios a través de los que se difunden. Lo que no cambia es el efecto que produce en quienes se ven afectados: mortificación y humillación.

Por otra parte, el **Derecho al Honor** es también asiduamente vulnerado mediante la utilización de Internet. De hecho, actualmente la *reputación online* forma parte del curriculum de las personas, dado que es cada vez más habitual que un empleador durante el proceso de selección de personal utilice buscadores (como Google, Yahoo) a fin de chequear la reputación de los postulantes en la web, así como para recabar mayor información sobre sus antecedentes.

“El concepto histórico de la palabra "reputación" sigue siendo el mismo, esto es, la opinión que los demás tienen sobre una determinada persona o compañía. La diferencia entre el concepto tradicional y el actual está dada porque, en el presente, hay millones de personas opinando al

4 "*Ponzetti de Balbín, Indalia c. Editorial Atlántida, S.A. s/ daños y perjuicios*", fallo del 11/12/1984, accedido en notasfallosconstitucionaluba.blogspot.com.ar

mismo tiempo y en muchos casos, en tiempo real” (Tomeo, 2012). Dicha situación, nos conduce a tener que cuidar nuestra reputación online.

Es necesario que los usuarios adviertan que tienen a su alcance una potente herramienta (Internet) que deben aprender a manejar con prudencia y plena conciencia de que cada publicación les puede traer aparejadas consecuencias lesivas para sus propios derechos personalísimos, así como los derechos de terceros. Nos encontramos ante el desafío de adquirir habilidades que nos permitan tener el control sobre ellas, antes de que otras personas, públicas o privadas, se valgan de ellas para controlarnos.

- **Afectación por parte de los Buscadores:** Podemos definir a los buscadores de Internet como herramientas indispensables al momento de utilizar la red de redes para buscar información, ya sea con fines educativos o laborales. En Argentina, se pueden citar como los más usados a Google, Yahoo! y Microsoft Live Search.

Sin embargo, en los últimos tiempos han sido objeto de crítica por parte de personas que se han visto injuriadas, y afectadas en su intimidad, imagen y reputación, al momento de ingresar su nombre en el motor de búsqueda. Esto se debe a que los buscadores de Internet retienen grandes volúmenes de datos de sus usuarios.

Numerosos modelos se sorprendieron al ver que su imagen, en los resultados de búsqueda, aparecía vinculada a sitios web de contenido sexual, erótico y pornográfico. Esta situación, las llevó a entablar demandas contra tales buscadores para que los mismos eliminen los contenidos agraviantes.

El problema es que en estos casos, la jurisprudencia fija soluciones diferentes. Esto sucede por la ausencia de una legislación clara al respecto, lo cual lleva a interpretaciones que son muchas veces contradictorias porque dependen de la postura que cada juez tenga sobre la materia. En su mayoría, coinciden en que el marco jurídico está dado por las disposiciones de derecho común sobre responsabilidad civil. La disidencia viene marcada por el tipo de responsabilidad civil que se les atribuye:

- A criterio de algunos jueces, a los buscadores se les imputa una **responsabilidad objetiva**, porque se trata de una cosa riesgosa que además realiza una actividad riesgosa en los términos del artículo 1113, segundo párrafo, última parte del Código Civil. Quienes adoptan esta postura, entienden que los buscadores no son sólo facilitadores de búsquedas sino también potenciadores del daño. De allí, que les han ordenado eliminar en forma definitiva de los

resultados de búsqueda: la imagen y/o el nombre de la persona vinculados con sitios web de contenido sexual, erótico y pornográfico⁵.

- Otros magistrados, en tanto, establecen que no resulta viable imputar responsabilidad objetiva al buscador de Internet, porque el mismo no contribuye a la generación del daño ni como autor ni como editor de los contenidos. Consideran aplicable la **responsabilidad subjetiva** por contenidos publicados por terceros cuando existe un obrar negligente de su parte, contemplada en los artículos 512, 1109 y conc. Código Civil⁶.

Teniendo en cuenta que los buscadores de Internet son utilizados en el mundo entero, lo ideal en este aspecto sería fijar reglas internacionales que garanticen la privacidad en la red de redes, logrando, por ejemplo, que una vez que los datos personales almacenados dejen de ser necesarios para las finalidades del servicio, los mismos sean borrados o cancelados.

La idea no es desalentar la utilización de Internet ni establecer límites a la libre circulación de la información, sino hacer un uso responsable de la red de redes que permita proteger los derechos propios y no violar los derechos ajenos.

Protección de Datos Personales

La marea de alteraciones que trajo consigo la expansión mundial de Internet ha impuesto un nuevo reto a los operadores jurídicos: ocuparse de desarrollar una legislación que regule la “Protección de los Datos Personales y la Intimidad de los usuarios” en relación a las modernas técnicas de recolección, almacenamiento, entrecruzamiento y transmisión de datos.

El agravamiento de la potencialidad dañosa que caracteriza a Internet hizo que se empezara a debatir acerca del “*derecho a la protección de datos*” o también denominado “*derecho a la autodeterminación informativa*”, que ha sido definida como “aquella parte de la legislación que protege el derecho fundamental de libertad, en particular el derecho individual a la intimidad respecto del procesamiento manual o automático de datos” (Hondius, 1983, pág. 105).

El mentado derecho, tiene como objeto inmediato la protección de los datos, pero como fin último, la tutela de un plexo de bienes jurídicos que son específicamente atacados por el tratamiento de datos. Entre tales bienes jurídicos están implicados tanto principios rectores de los

⁵ Cámara Nacional de Apelaciones en lo Civil de la Capital Federal: Sala J. “Krum: Andrea Paola c/ Yahoo de Argentina S. R. L y otro s/daños y perjuicios” Expte. N° 84.103/2007, fallo del 31/08/2012, accedido en <http://www.paradigmadelderecho.com.ar/web/?p=4285>

⁶ Cámara Nacional de Apelaciones en lo Civil, Sala D, "Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y Perjuicios", Expte. N° 99.620/2006, fallo de agosto de 2010, accedido en www.hfernandezdelpech.com.ar/

derechos humanos: libertad, dignidad e igualdad, como múltiples derechos fundamentales: intimidad, identidad, honor, propiedad sobre los datos, etcétera (Puccinelli, s/f).

En Argentina, con la reforma constitucional de 1.994 se incorporó el Habeas data en el Artículo 43, tercer párrafo, el cual expresa: "*Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística*".

"El art. 43 CN no utiliza ni menciona la expresión "*habeas data*". La omisión se debe a que la ley declarativa de la necesidad de reforma constitucional no hizo referencia al habeas data, y solamente habilitó enmiendas para incorporar el *habeas corpus* y el *amparo*. De ahí que el constituyente haya dado cauce al habeas data a través de la acción de amparo" (Bidart Campos, 2003, pág. 310).

"El habeas data significa que cada persona "*tiene sus datos*". No hay duda de que el objeto tutelado coincide globalmente con la intimidad o privacidad de la persona, ya que todos los datos a ella referidos que no tienen como destino la publicidad, o la información a terceros, necesitan preservarse" (Bidart Campos, 2003, pág. 310).

"La norma constitucional ampara los derechos de las personas a *conocer* sus datos y la *finalidad* de su almacenamiento; y eventualmente a solicitar medidas, tales como la *supresión, rectificación, confidencialidad o actualización*, sobre el registro que de ellos se hubieren efectuado en bancos públicos o privados proveedores de informes. Tanto la persona humana como las personas jurídicas están amparadas por la disposición constitucional" (Gelli, 2009, pág. 641).

Conforme lo establece la norma constitucional, los registros o bancos de datos pueden ser "*públicos*" (debemos entender los existentes en los organismos del Estado de cualquier naturaleza) o "*privados destinados a proveer informes*" (aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, sea a título oneroso o gratuito. Por ejemplo: las empresas o personas individuales dedicadas a recolectar información personal para suministrarla a sus clientes).

Entendemos que debe efectuarse una interpretación amplia acerca del alcance de la garantía prevista en el art. 43 tercer párrafo CN permitiendo que los usuarios dispongan de la Acción de

Amparo Especial para conocer y en su caso solicitar la supresión, rectificación, confidencialidad o actualización de sus datos personales a las empresas responsables de bancos de datos automatizados. Lo contrario nos llevaría a desvirtuar el fin último al que responde la garantía, cual es la salvaguarda del derecho a la intimidad personal y familiar.

En consecuencia, creemos que la garantía del hábeas data debe interpretarse con una amplitud y flexibilidad tal, que admita la tutela de nuevos bienes jurídicos, derechos y situaciones que se vayan presentando en los casos concretos.

La Ley 25.326 de Protección de los Datos Personales

En Argentina, la **Ley 25.326 de “Protección de los Datos Personales y Hábeas Data”** sancionada el 4 de octubre de 2000, vino a cubrir el vacío legislativo existente desde la Reforma Constitucional de 1994 que instituyó el hábeas data en el Art. 43 tercer párrafo CN.

La Ley 25.326 está destinada a regular “la protección integral de los datos personales asentados en bancos de datos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre” (Art. 1º).

La misma consagra una serie de derechos en favor de los titulares de los datos, a saber: *Derecho de Información; Derecho de Acceso; Derecho de rectificación, actualización o supresión;* y el *Derecho a la impugnación de valoraciones personales.*

Al mismo tiempo, establece una serie de obligaciones precisas para los responsables de bases de datos personales: entre ellas, tienen el deber legal de inscribirlas en un registro especial a cargo de la **Dirección Nacional de Protección de Datos Personales**, organismo dependiente del Ministerio de Justicia creado para velar por el cumplimiento de la ley y aplicar sanciones (tales como apercibimientos, multas y la posibilidad de suspender o clausurar las bases de datos).

Desde la óptica de la Ley 25.326 las Bases de Datos automatizadas, formadas a partir de la recolección de datos personales efectivizada a través de Internet, no cumplen con las siguientes obligaciones legales:

✘ En general, se trata de bases de datos que no se encuentran debidamente **inscriptas** y que por ende, no cumplen con los principios y reglamentaciones que establece la ley al efecto (art. 3).

✘ No se informa al titular el hecho de que sus datos están siendo recolectados. En consecuencia, se lo priva lisa y llanamente de los derechos de información, acceso, rectificación, actualización o supresión que la ley le garantiza.

✘ No se cumple con el **deber de informar** previamente al titular en forma expresa y clara: la finalidad para la que serán tratados sus datos y quiénes pueden ser sus destinatarios; la existencia del banco de datos electrónico y la identidad y domicilio de su responsable; la posibilidad de ejercer los derechos de acceso, rectificación o supresión; etc. (art. 6)

✘ El titular de los datos no efectúa un **consentimiento libre, expreso, informado y por escrito** que exige la ley (art. 5). “Se trata del pilar del sistema de protección de datos personales, toda vez que constituye la condición justificante de las operaciones de tratamiento a que pueden ser sometidos los datos, sin la cual las mismas quedan teñidas de ilicitud” (Peyrano, 2003). Su importancia radica en que constituye el medio a través de la cual el interesado tiene oportunidad de elegir el nivel de protección que le dará a la información sobre su persona. Consideramos que es un buen criterio de la ley exigir un consentimiento de tales características como recaudo de licitud pero las hipótesis excluidas son tan amplias que tienden a desvirtuarlo.

Sin embargo, el consentimiento otorgado con las características antes mencionadas es poco habitual en nuestros días. Ocurre que al contratar servicios en la web (utilizar una página, un blog, una red social, efectuar compras online, etc.) frecuentemente se nos presentan términos y condiciones del sitio y políticas de privacidad que finalizan con un “ACEPTAR”. De este modo, se pretende dar por configurado el consentimiento de los usuarios.

La naturaleza jurídica del contrato que rige la relación jurídica obligacional entre la empresa titular del sitio web y el usuario es la de un **“Contrato por Adhesión”**, el cual envuelve un consentimiento sin deliberaciones previas al aceptarse una fórmula preestablecida. Una de las problemáticas jurídicas que plantean estos contratos es en cuanto a la verdadera configuración o no del **“consentimiento informado”** de los usuarios.

Los términos y condiciones son textos extensos y complejos que, lejos de buscar garantizar los derechos de los usuarios y la seguridad en sus datos, sólo constituyen un instrumento diseñado por las empresas para resguardar su patrimonio ante posibles demandas por daños y perjuicios: ésa es la triste realidad. Además, los usuarios ceden derechos plenos e ilimitados (sin saberlo, claro está) sobre todos aquellos contenidos propios que alojen en la plataforma, de manera que pueden ser explotados económicamente.

En consecuencia, de la suscripción de contratos de adhesión online se deriva la imposición de cláusulas a los usuarios que implican constantes violaciones a sus derechos personalísimos por parte de las grandes empresas que dominan la Red.

✖ Los datos recolectados no son destruidos (pese a la prescripción del art. 4 inc 7) dado que los fines son abiertos y al no informarse a su titular puede que nunca dejen de ser necesarios a criterio de las grandes empresas (como las publicitarias). Prueba de ello, lo constituyen las cesiones de datos a terceros para fines distintos.

✖ Cada vez que se dan a conocer **datos sensibles** de personas identificables se está violando la **prohibición legal** de formar archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles (art. 7°).

✖ Por tratarse de bases de datos no registradas no es posible comprobar si se cumplen las **condiciones técnicas de integridad y seguridad** que exige la ley (art. 9).

✖ La **cesión de datos** no estaría amparada por la ley dado que al no conocerse claramente cuáles son los fines que persiguen cedente y cesionario, no puede saberse si se relacionan con un interés legítimo o no. Además, no se cumple con el recaudo de solicitar el previo consentimiento del titular de los datos y de informarle la finalidad de la cesión e identificar al cesionario (art. 11).

✖ Por último, al no existir conocimiento por parte de la mayoría de los titulares de que sus datos personales están siendo recopilados y sometidos a tratamiento, la Acción de Hábeas Data deviene totalmente **INEFICAZ**. Incluso, en el supuesto de que llegaren a advertirlo, resulta difícil cumplir con los requisitos de la demanda exigidos por el art. 38 de la ley, a saber: *“...individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo...”*

De lo expuesto, surge a simple vista el carácter **ILÍCITO** que yace en la explotación de datos personales perpetrada a través de Internet, como así también la ineficacia de las acciones concedidas por la legislación nacional a los titulares de los datos, cuyos derechos están siendo ferozmente atacados desde distintos frentes.

Para concluir con éste análisis, queremos dar cuenta de que, a nuestro humilde entender, la sanción de la Ley 25.326 si bien logró saldar un vacío legal en torno al tratamiento de datos personales en el derecho argentino, resulta insuficiente para asegurar la operatividad de la garantía prevista en el Art. 19 CN. Esto se debe a que el avance de la tecnología superó las previsiones efectuadas por aquella ley, por lo que la intimidad continúa en riesgo, sobre todo en

lo que a las comunicaciones electrónicas se refiere. Se trata de nuevas situaciones que arroja el mundo virtual y que están lejos de hallarse contempladas por la ley argentina.

Creemos imprescindible el consenso internacional para regular este fenómeno y luchar por la salvaguarda de los derechos humanos, garantizando principalmente al hombre la posibilidad de “una vida pública y una vida privada”, cuyos contornos puedan ser delimitados por el propio individuo. La privacidad es **intrínseca al concepto de libertad**. Los seres humanos no somos únicamente criaturas sociales, somos también **seres privados!!!**

Conclusión

Sin lugar a dudas, abordar las nuevas situaciones que suscita Internet en su totalidad, en tanto nuevo escenario de constantes y mutantes formas de afectación de una multiplicidad de derechos, resulta una misión imposible o al menos dificultosa.

El problema no sólo yace en la actitud asumida por las empresas que buscan obtener lucro sin detentar límites, sacando frutos a los vacíos legislativos reinantes; sino en la falta de toma de conciencia real por parte de los usuarios del valor que tienen sus datos personales en la sociedad actual.

La regulación jurídica existente en nuestro país si bien cumplió con los objetivos propuestos al tiempo de su sanción, está lejos de dar respuesta a los nuevos conflictos que ocasiona la Red. Es claro que, la reforma de la legislación vigente sería el camino óptimo. No obstante, ante la inminencia y magnitud que han adquirido las modernas formas de afectación de derechos personalísimos, consideramos que flexibilizar la interpretación del Habeas Data sería de momento una solución factible.

Por último, creemos conveniente que los datos personales subidos a Internet tengan “*fecha de vencimiento*”, es decir, puedan ser eliminados en algún momento, por más utópico que ello parezca. A tal fin, una alternativa viable podría ser la consagración del llamado “**Derecho al Olvido**”, del que ya han efectuado alguna alusión especialistas informáticos. Este derecho otorgaría a los ciudadanos la potestad de reclamar que, transcurrido cierto tiempo, información personal sobre ellos e irrelevante para la comunidad sea eliminada de la web.

Ante este panorama, creemos que el mayor peligro se despliega en torno al modo con que las personas vamos naturalizando prácticas que suponen una directa y avasallante intromisión en nuestra esfera más íntima, sobre todo porque tal actitud podría decantar en la conformación de

sociedades en las que se predique un concepto devaluado de la privacidad.

Estamos convencidas de que es fundamental la salvaguarda del ámbito privado por su intrínseca vinculación con el desarrollo de la personalidad, la autodeterminación y construcción de la propia esencia y dignidad. La privacidad nos define como seres humanos, nos diferencia de las demás especies que habitan el planeta Tierra. Si perdemos tal ámbito, perdemos también un poco de humanidad...

Bibliografía

BIDART CAMPOS, GERMÁN J. (2003): *Tratado Elemental de Derecho Constitucional Argentino*, Tomo II-A. Nueva Edición ampliada y actualizada a 2002-2003, Sociedad Anónima Editora, Comercial, Industrial y Financiera.

CAO AVELLANEDA, JAVIER, *Identidad Digital y Reputación online, la gestión de la e-privacidad*, publicado en el sitio web www.informaticalegal.com.ar; consultado el 8 de febrero de 2013.

FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, “Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red”, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica Núm. 154.

GELLI, MARÍA ANGÉLICA, (2009): *Constitución de la Nación Argentina. Comentada y Concordada*, Tomo I. Buenos Aires: Editorial LA LEY.

GIULIANO, DIEGO ALBERTO (2000), “El "habeas data" y la explotación de los datos personales: el caso argentino”, publicado en *Cuadernos Constitucionales de la Cátedra Fadrique Furio Ceriol*, N° 32. Departamento de Derecho Constitucional y Ciencia Política y de la Administración de la Universidad de Valencia (España).

GONZALEZ FREA, LEANDRO, Aspectos Legales y Normativos de las Redes Sociales Un breve Análisis Jurídico de las Redes Sociales en Internet en la óptica de la normativa Argentina, accedido a través de la web: www.gonzalezfrea.com.ar, consultado el 20 de enero de 2013.

HONDIUS F. (1983): “A decade of international Data Protection”, *Netherlands of International Law Review*, (N° 2, vol 30, 1983).

PEYRANO, GUILLERMO (2003), “El principio del consentimiento en el "sistema de protección de los datos personales". Condiciones de validez y posibilidad de revocación del consentimiento prestado. El derecho de oposición”, publicado en *Coleccion Zeus - Doctrina boletín* N° 7216, 7 de Julio de 2003.

PEYRANO, GUILLERMO (2002), “Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico”, publicado en *El Derecho- Boletín* N° 10.651, 13 de diciembre de 2002.

PUCCINELLI, OSCAR RAÚL, “Acerca de la evolución y actual autonomía de los derechos “de” y “a” la protección de datos”, publicado en *Revista Internacional de Administración Pública*.

SAL PAZ, JULIO CÉSAR, “Notas sobre las Tecnologías de la Información y de la Comunicación”, *Sociedad y Discurso*, Universidad de Aalborg, número 17: 44-72, publicado en el sitio web: http://vbn.aau.dk/files/62701961/SyD17_sal.pdf; consultado el 22 de noviembre de 2012.

TOMEIO, FERNANDO, “Etiquetar una foto en Facebook puede afectar derechos personalísimos”, publicado en La Nación, accedido a través de la web: www.lanacion.com.ar; consultado el 8 de enero de 2013.

TOMEIO, FERNANDO, "Striptease digital y datos personales", publicado en La Nación, accedido a través de la web: www.lanacion.com.ar; consultado el 8 de enero de 2013.

UICICH, Rodolfo Daniel (2007), "La cuestión de la privacidad de los datos en Internet", en *La Revista de la Protección de Datos de la Comunidad de Madrid*, N° 30 - 30 noviembre 2007, accedido través de la web: www.madrid.org, consultado el 8 de febrero de 2013.

UICICH, RODOLFO DANIEL (2009): *El Derecho a la Intimidad en Internet y en las comunicaciones electrónicas*, Buenos Aires: editorial Ad-Hoc.