

**Universidad Nacional de La Pampa**  
**Facultad de Ciencias Económicas y Jurídicas**



**Seminario sobre Aportaciones**  
**Teóricas y Técnicas Recientes**

**“TRÁFICO DE DATOS PERSONALES:**  
**Su Afectación a los Derechos**  
**Personalísimos”**

**Asignatura: Derecho Constitucional**  
**Director del Seminario: Jorge Cañón**  
**Estudiantes: Ferrero, Eliana Mariel; Schutz, Anabella**  
**Año que se realiza el trabajo: 2013**

**“TRÁFICO DE DATOS PERSONALES: Su afectación a los  
Derechos Personalísimos”**

*“Nunca antes como en la actualidad ha sido posible saber tanto de tantas personas sin que ellas mismas lo sepan. En nada exagero al afirmar que del respeto a la protección de datos depende en gran medida el futuro de una sociedad en libertad, respetuosa con los derechos de las personas y en particular de su dignidad, pues no podemos olvidar que cuando alguien trata ilegítimamente nuestros datos personales está manipulando nuestra identidad y, en consecuencia, está jugando con nuestra dignidad”*

**José Luis Piñar**

**Director de la Agencia Española de Protección de Datos**

## ÍNDICE GENERAL

<b>INTRODUCCIÓN.....</b>	<b>4</b>
<b>CAPÍTULO I: LA SOCIEDAD DE LA INFORMACIÓN...6</b>	
<b>CAPÍTULO II: PLANO CONCEPTUAL Y REGULACIÓN NORMATIVA DE LOS DERECHOS A LA INTIMIDAD, AL HONOR Y A LA IMAGEN PERSONAL.....</b>	<b>14</b>
<b>CAPÍTULO III: TRÁFICO DE DATOS PERSONALES..</b>	<b>37</b>
<b>CAPÍTULO IV: REDES SOCIALES.....</b>	<b>61</b>
<b>CAPÍTULO V: AFECTACIÓN DE LOS DERECHOS A LA INTIMIDAD, AL HONOR Y A LA IMAGEN PERSONAL.....</b>	<b>75</b>
<b>CAPÍTULO VI: PROTECCIÓN DE DATOS PERSONALES.....</b>	<b>97</b>
<b>CONCLUSIÓN.....</b>	<b>169</b>
<b>BIBLIOGRAFÍA.....</b>	<b>172</b>

## INTRODUCCIÓN

La vertiginosa evolución que han tenido las Tecnologías de la Información y la Comunicación (TICs) en los últimos años a escala mundial, borrando las fronteras de tiempo y espacio, llegando a penetrar en el ámbito de nuestro hogar y formando parte de nuestra vida cotidiana, nos llevó a reflexionar sobre la importancia de tomar conciencia de que se están produciendo cambios abismales que nos obligan a adaptarnos a ellos; pero nuestro desafío es que esa adaptación no sea pacífica-receptiva, sino reflexiva y crítica.

Como estudiantes de Derecho, advertimos el fuerte impacto que está generando Internet sobre nuestros derechos fundamentales, principalmente sobre el Derecho a la Intimidad, al Honor y a la Imagen personal, los cuales están siendo atacados a través una nueva práctica: “El Tráfico de Datos Personales”.

Los Datos Personales se han convertido en una mercancía que cotiza a un alto valor en el mercado, para cuya captación y transmisión se utilizan tecnologías de diversa índole, al mismo tiempo que se manipula la información que los usuarios proporcionan a páginas web,

blogs, redes sociales, sin tomar conciencia de los perjuicios que puede ocasionarles.

Las grandes empresas o grupos económicos utilizan esos datos para conocer los gustos, preferencias y hábitos de consumo de la población buscando liderar el mercado, sin detentar ningún tipo de valla ética...

El estudio que presentamos busca resaltar la trascendencia que tiene para los seres humanos la preservación de un ámbito privado, un ámbito de reserva, en el que nada ni nadie pueda inmiscuirse, cuya garantía reclama la sanción de leyes que protejan los datos personales frente a los nuevos peligros que suponen los progresos técnicos, así como la incorporación o rediseño de mecanismos que brinden una respuesta rápida a aquellas personas que vean conculcados sus derechos como consecuencia de la manipulación de datos efectivizada a través de Internet.

Asimismo, consideramos de vital importancia que las personas comencemos a adquirir habilidades relacionadas con el manejo de las TICs que nos permitan tomar las precauciones necesarias antes de lanzar información personal a la Red.

## CAPÍTULO I: LA SOCIEDAD DE LA INFORMACIÓN

En el devenir de la historia de la humanidad el desarrollo de diversidad de tecnologías ha sido el puntapié de grandes cambios sociales, económicos y culturales. Tal lo que ocurrió con las dos grandes revoluciones tecnológicas que marcaron la historia contemporánea: la invención de la “máquina de vapor” y del “motor eléctrico”.

En la actualidad, estamos inmersos en lo que podría individualizarse como la tercera revolución: 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”.

Somos testigos de la emergencia de una nueva sociedad civil que desborda las fronteras de los Estados-Nación y funciona en unidad de tiempo real y a escala global<sup>1</sup>.

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 que han sido definidas como: “conjunto de procesos y productos derivados de las nuevas herramientas -hardware y software-, soportes y canales, relacionado con el almacenamiento, procesamiento y transmisión digitalizados de la información, que permite su adquisición, producción, tratamiento, comunicación, registro y presentación, en forma de voces, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética”<sup>2</sup>.

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

---

<sup>1</sup> PORRAS MARTINEZ, JOSÉ IGNACIO, “Los cambios tecnológicos y sociales que posibilitan la Organización en Red”, éste artículo fue presentado en forma de ponencia dentro del Ciclo de Conferencias del Centro de Estudios del Comportamiento Organizacional (CECO), Universidad Bolivariana, el 3 de abril de 2001 y publicado en Revista de la Universidad Bolivariana Volumen 1 Número 2, 2001.

<sup>2</sup> 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](http://vbn.aau.dk/files/62701961/SyD17_sal.pdf).

televisión y la telefonía convencional- y otro, encarnado por las 'Tecnologías de la Información' (TI) -caracterizadas por la digitalización de las técnicas de registro de contenidos (informáticas, de comunicación, telemáticas y de interfaces)<sup>3</sup>.

Por su parte, el estadio actual de desarrollo de la civilización humana ha sido denominado "**Sociedad de la Información**", aunque también se han utilizado otras expresiones como "Sociedad del conocimiento", "Sociedad Digital", "Era Digital", "Sociedad en Red", etc.

La Sociedad de la Información 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. "La información de todo tipo- asevera Alvarez-Cienfuegos- se ha convertido en un *bien de consumo*; hay auténtica demanda social de información; el político; el empresario; el comerciante necesitan para desarrollar su trabajo cada

---

<sup>3</sup> 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](http://vbn.aau.dk/files/62701961/SyD17_sal.pdf).



día más información, incluso, el mismo ciudadano, en su dimensión más anónima, invierte gran parte de su ocio en consumir información”<sup>4</sup>.

La información es la materia prima y el conocimiento es el producto<sup>5</sup>. De esa información, una de las más valiosas es la que alude a los “**Datos de carácter Personal**”, cuyo análisis será motivo de otro capítulo.

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.

Internet, que podría definirse como “Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación”<sup>6</sup>, ha producido un cambio radical en la forma de transmitir la información. Para ello se utilizan distintas herramientas, siendo las más habituales:

1. La *World Wide Web* (representa la parte multimedia de Internet, es un inmenso conjunto de documentos electrónicos con

---

<sup>4</sup> 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, página 21.

<sup>5</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, “op cit” página 22.

<sup>6</sup> Diccionario de la Real Academia Española, vigésima segunda edición.

información digitalizada<sup>7</sup>) a través de ésta y de sus sitios podemos publicar y recuperar documentos, imágenes, sonidos, videos, etc. Navegar por sus páginas es acceder a un mundo fantástico de conocimientos, novedades e información.

2. El *electronic mail* (e-mail o correo electrónico), nuestras cartas, mensajes, postales y fotos que pueden ser enviadas y difundidas en escasos segundos a uno o infinitos receptores a quienes les llegará inmediatamente, por lo que también puede recibir la respuesta en el tiempo que tarde el remitente en enviarla.
3. El *Internet Relay Chat* (IRC), herramienta mediante la cual podemos dialogar en tiempo real.
4. Los *usenet newsgroups* o grupos de noticias, que son bases de mensajes agrupados por temas, y
5. El *File Transfer Protocol* (FTP), que nos permite enviar archivos de datos por Internet, de cualquier magnitud y formato, y que conlleva el beneficio adicional de permitir copias de seguridad en otros equipos distantes y evitar así el soporte magnético para el back up<sup>8</sup>.

---

<sup>7</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, "op cit" página 24.

<sup>8</sup> UICICH, RODOLFO DANIEL, El Derecho a la Intimidad en Internet y en las comunicaciones electrónicas, editorial Ad-Hoc, Buenos Aires, 2009, página 78.

Vale decir, que no constituye el objeto del presente trabajo el dar una conceptualización y explicación detallada de cómo funciona Internet, razón por la cual las nociones dadas anteriormente son meramente orientadoras.

Ahora bien, esta casi mágica posibilidad de comunicarnos de variada forma ha generado un flujo de información de magnitud increíble, a la vez que impresionante, así como una fuente de recursos obtenidos con la venta masiva de servicios y productos de la más inimaginable diversidad<sup>9</sup>.

Lo que nos interesa destacar aquí es que Internet ha permitido la recolección, almacenamiento y transmisión de datos prácticamente al instante, así como la generación de bases de datos eficientes, rápidas y relativamente económicas. Con ello se ha desencadenado una circulación de datos que ocasiona una lesión al derecho a la intimidad y/o una intromisión a la vida privada de las personas cuyos antecedentes han sido recopilados sin su consentimiento, y en muchos casos sin siquiera su conocimiento.

De modo que, si bien es cierto que las TICs han traído consigo evidentes **ventajas** en el acceso a la información, al permitir un acceso

---

<sup>9</sup> UICICH, RODOLFO DANIEL, “op cit” página 78.

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, puesto que facilitan la interconexión entre los individuos e instituciones a nivel mundial. No obstante, no podemos quedarnos solo con su lado positivo siendo que, tal como afirma José Julio Fernández Rodríguez: “no todo lo que rodea Internet son luces, ya que también se localizan sombras todavía sin disipar”<sup>10</sup>.

Es por ello, que consideramos de vital importancia que la sociedad toda comience a tomar conciencia de que dichas ventajas esconden un lado oscuro en lo que respecta al uso y abuso de Internet en particular, que consiste en la **afectación de derechos personalísimos** como son el **derecho a la intimidad, el derecho al honor y el derecho a la imagen**, así como la **reducción del ámbito privado** de los individuos. Un ámbito en el que la libre determinación y la no injerencia de terceros, debiera ser tan infranqueable como el propio Derecho a la Vida.

---

<sup>10</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, “op cit” página 10.

En definitiva, la Red abre un frente de redefiniciones y reconstrucciones que afectan a diversas categorías jurídico-sociales. Ello es todavía un proceso en marcha que nos sitúa, al menos de momento, en el terreno de lo provisional e impone nuevos retos a los operadores jurídicos. Ante los mencionados retos, hay que responder con prontitud y corrección, para seguir cumpliendo, con eficacia y justicia, con el fin de regular la vida en sociedad<sup>11</sup>.

---

<sup>11</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, "op cit" página 24.

## **CAPITULO II: PLANO CONCEPTUAL Y REGULACIÓN NORMATIVA DE LOS DERECHOS A LA INTIMIDAD, AL HONOR Y A LA IMAGEN PERSONAL**

El caudal 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). Ésta situación ha desencadenado la constante afectación de derechos personalísimos en general y del Derecho a la Intimidad y a la Privacidad, el Derecho a la Imagen y el Derecho al Honor de las personas en particular.

Con el propósito de abordar con mayor claridad la problemática que despliega la afectación de estos derechos, brindaremos a continuación algunas nociones conceptuales y su regulación normativa en el derecho argentino, que entendemos serán de utilidad para la mejor comprensión de la temática a desarrollar en la presente investigación.

Si quisiéramos definir brevemente a los derechos personalísimos o de la personalidad, podríamos decir que son aquellos que están íntimamente unidos a la persona, nacen con ella, y no pueden separarse en toda su existencia, a riesgo de perderla o denigrarla. Se los precisa como las prerrogativas de contenido extrapatrimonial, inalienables, perpetuas y oponibles erga omnes, que corresponden a toda persona por su condición de tal, desde antes de su nacimiento y hasta después de su muerte, y de la que no puede ser privada por la acción del Estado ni de otros particulares.

Respecto a su naturaleza jurídica, algunos autores sostienen que no constituyen derechos subjetivos sino que importan presupuestos jurídicos de la personalidad. Sin embargo, para la opinión predominante se trata de verdaderos derechos subjetivos.

Esta categoría de derechos presenta determinados caracteres, los cuales, según Santos Cifuentes, son:

a) Son **derechos innatos**, debido a que nacen con el sujeto mismo. Pertenecen al hombre por su sola condición de persona humana, siendo indiferente lo que disponga o no al respecto el derecho objetivo.

b) Son **derechos vitalicios**, ya que pertenecen a la persona durante toda su existencia, no faltando en ningún instante de la vida.

c) Son **derechos necesarios** por cuanto no pueden faltarle a la persona, sin perjuicio de que en ciertas ocasiones su ejercicio pueda ser limitado por la autoridad pública (por ejemplo, en el caso de una condena penal de prisión se privaría el ejercicio al derecho de libertad ambulatoria).

d) Son **derechos esenciales**, ya que no le pertenecen al hombre por una circunstancia ajena o externa sino que se trata del mínimo indispensable, básico, para el contenido de la personalidad humana.

e) Son **derechos de objeto interior**, debido a que al ser manifestaciones de la persona se encuentran íntimamente vinculados a ella y no pueden ser captados sin atender a la unidad compuesta del hombre.

f) Son **derechos inherentes**, puesto que son intransmisibles por no ser posible escindirlos de la persona a la que pertenecen. De ello resulta que los derechos personalísimos son irrenunciables.



g) Son **extrapatrimoniales**, ya que no son susceptibles de apreciación o medición pecuniaria. De todos modos hay que tener en cuenta que, no obstante este carácter extrapatrimonial, la lesión de los derechos personalísimos tiene repercusiones económicas ya que si se atenta contra ellos, la víctima tiene la facultad de exigir su reparación in natura, y si la reparación en especie fuera imposible, la obligación de resarcir se resuelve en el pago de una suma de dinero.

h) Se trata de **derechos relativamente indisponibles** ya que no es posible venderlos ni transmitirlos. Son derechos inenajenables, inembargables, intransferibles, imprescriptibles e inejecutables. Sin embargo afirmamos que esta indisponibilidad es "relativa" porque es posible alterarlos, transitoria y parcialmente.

i) Son **derechos absolutos** en el sentido de que son oponibles erga omnes a todos los miembros de la comunidad y no sólo a los particulares, sino también frente al Estado.

j) Los derechos personalísimos son **derechos privados** por cuanto se colocan en el campo del comportamiento de los particulares<sup>12</sup>.

---

<sup>12</sup> CIFUENTES, SANTOS, "Elementos de Derecho Civil Parte General", editorial Astrea, Buenos Aires, 1997, páginas 150 y siguientes.

Por otra parte, y ya adentrándonos en una posible clasificación, muchos autores sostienen que prevalece el criterio de considerar que existe una variedad diferenciada de derechos personalísimos que responden a la protección de distintos bienes o manifestaciones interiores de la persona. Así, encontramos:

a) Derechos a la integridad física. Comprende el derecho a la vida, la salud y el destino final del cadáver.

b) Derecho de libertad. Aquí, se atiende al problema físico (el movimiento, la locomoción) y también lo concerniente a la expresión de las ideas, la realización de actos o negocios.

c) Derechos de la integridad espiritual. Comprenden el honor, la imagen, la intimidad o vida privada y la identidad.

Un reflejo de la magnitud que revisten los derechos personalísimos se sintetiza en la siguiente frase que Germán Bidart Campos expone: “Toda vida, en cuanto vida, es valiosa. El valor de la vida humana no depende de quien sea y cómo sea cada ser humano: por más degradado, por más delincuente, por más vil que sea un hombre, su vida – como vida humana – vale en sí misma”.

Ya inmersos en el conocimiento y la trascendencia de la categoría a la cual pertenecen, debemos retomar la idea expuesta al inicio del presente capítulo: comprender y defender la importancia del Derecho a la Intimidad, el Derecho al Honor y el Derecho a la Imagen personal, los cuales se desarrollarán a continuación.

### Derecho a la Intimidad

El término íntimo viene de intimus, que significa "lo más interior". Según la definición brindada por el Diccionario de la Real Academia Española, intimidad significa "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"<sup>13</sup>. La intimidad corresponde al ámbito psicológico e inconmensurable del individuo, comprende su personalidad, sus valores morales y religiosos, sus tendencias sexuales y amorosas, sus orientaciones ideológicas.

Como dijimos anteriormente, el derecho a la intimidad es un derecho personalísimo: se lo define como el derecho que tiene todo individuo de determinar por su cuenta, cómo y en qué medida, las

---

<sup>13</sup> Diccionario de la Real Academia Española, vigésima segunda edición.

informaciones que le atañen puedan ser comunicadas a otras personas. Es un derecho que protege la esfera más íntima de la persona, y se halla estrechamente ligado a la protección de la dignidad del individuo.

Según Humberto Quiroga Lavié, el derecho a la intimidad "es un derecho personalísimo que permite sustraer a las personas de la publicidad o de otras turbaciones a su vida privada, el cual está limitado por las necesidades sociales y los intereses públicos. Este derecho implica el respeto a la personalidad humana, del aislamiento del hombre, de lo íntimo de cada uno, de la vida privada, de la persona física, innata, inherente y necesaria para desarrollar su vida sin entorpecimientos, perturbaciones y publicidades indeseadas".

Para Miguel Padilla el derecho a la intimidad "es el derecho que tienen los individuos, los grupos y las instituciones, de determinar por su cuenta cómo y en qué medida las informaciones que les atañen pueden ser recolectadas, tratadas y, eventualmente, comunicadas a otras personas"<sup>14</sup>.

Por su parte, la Corte Suprema de Justicia de la Nación proclamó que el derecho a la intimidad ampara la autonomía individual

---

<sup>14</sup> PADILLA, MIGUEL M., "Bancos de Datos y Acción de Hábeas Data", Editorial Abeledo Perrot, Buenos Aires, página 31.

integrada por sentimientos, hábitos, costumbres, relaciones familiares, posición económica, creencias religiosas, salud mental y física y todos los datos y hechos que integran el estilo de vida de una persona que la comunidad considera reservadas al individuo y cuyo conocimiento o divulgación significa un peligro para la intimidad<sup>15</sup>.

Asimismo, es importante destacar que se ha sostenido que el derecho a la intimidad está protegido y de esta protección gozan tanto las personas intachables, como también cualquiera que sufra un ataque injusto. Tal como expone Orgaz, "la protección de la vida privada no solamente defiende a la persona contra las falsedades que puedan menoscabar su reputación, sino también contra la innecesaria revelación de sus miserias y flaquezas"<sup>16</sup>.

### Regulación Normativa

---

<sup>15</sup> PALAZZI, PABLO ANDRÉS, en el artículo "El Hábeas Data en el Derecho Argentino". Por Pablo Andrés Palazzi. Abogado. Coordinador del Posgrado en Derecho de la Alta Tecnología. Universidad Católica Argentina Facultad de Derecho. Profesor de Derecho Constitucional UCA (Argentina).

<sup>16</sup> Cit por ORGAZ, A., Personas individuales, Buenos Aires, 1946, cit en LLAMBÍAS, J.J., Tratado de Derecho Civil Parte General I, editorial Perrot, 1967, página 275.

El hombre tiene la libertad de dar a conocer de sí mismo, a los demás, lo que considere pertinente, derecho que parece difícil de ejercer en estos tiempos si tenemos en cuenta el avasallante desarrollo de la tecnología. Por eso es importante destacar que el hombre como titular de derechos, debe defenderse tanto de las intromisiones indebidas del Estado como de los ataques a la intimidad ocasionados por otros individuos. Ante esto debemos preguntarnos: ¿Protege la ley Argentina la intimidad de una persona? La respuesta a esta pregunta es afirmativa: el Derecho es el que se ocupa, a través de sus leyes, de evitar la injerencia de terceros a la información que el hombre estime no comunicable.

\* En principio, el derecho a la intimidad e desprende del de privacidad garantizado en el artículo 19 de nuestra Constitución Nacional, el cual en su primera parte reza: "Las acciones privadas de los hombres que de ningún modo ofendan el orden ni la mora pública, ni perjudiquen a un tercero, están reservadas sólo a Dios, y exentas de la autoridad de los magistrados...". De aquí, se establece que el derecho a la intimidad es el que garantiza a su titular el desenvolvimiento de su vida y de su conducta dentro de aquel ámbito privado, sin injerencias que puedan provenir de la autoridad o de terceros, y en tanto dicha

conducta no ofenda al orden público y a la moral pública, ni perjudique a otras personas.

\* A su vez, la Constitución Nacional, reformada en el año 1994, otorgó rango constitucional, en su artículo 75 inciso 22, a documentos internacionales que a través de sus artículos reconocen la protección de la intimidad como un derecho del hombre. Entre ellos, encontramos:

- El artículo 12 de la Declaración Universal de los Derechos del Hombre, el cual establece que "...Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques..."

- El artículo 17 del Pacto de las Naciones Unidas relativo a los Derechos Civiles y Políticos que sostiene que "... Nadie será objeto de injerencias arbitrarias o legales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su hora y reputación..."-.

- El artículo 11.2 del Pacto de San José de Costa Rica dispone sobre el derecho a la intimidad que "...Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia,

en su domicilio o en su correspondencia, ni de ataques ilegales a su honra reputación..."

\* Por su parte, y adentrándonos ya en lo dispuesto por el Código Civil respecto a este derecho, encontramos su artículo 1071 bis, el cual se suma a las normas anteriormente mencionadas para proteger la esfera de la intimidad, pero de una manera un tanto más específica. El mismo establece "...El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación...". Así, se ha dicho que este artículo contempla la revelación de secretos o de intromisiones en lo reservado e íntimo y los ataques u ofensas que, atormentando a otros en sus costumbres o sentimientos, perturban de cualquier modo su intimidad. Además es interesante, tal como se explica en el Código Civil comentado de Bueres, que la doctrina



uniformemente ha entendido que la fórmula genérica que contiene este artículo permite una ágil adaptación de la legislación a las nuevas circunstancias: esto es, los adelantos técnicos en los aparatos de escucha y obtención de imágenes y los avances en el campo de la informatización e Internet, que hacen difícil evitar las injerencias<sup>17</sup>, tal como veremos en los próximos capítulos del presente trabajo.

\* Vale destacar que con la reforma constitucional de 1994 se incorporó expresamente a la Constitución Nacional el artículo 43, que le da a los ciudadanos la posibilidad de interponer la acción de habeas data para que puedan tomar conocimiento de sus datos personales que consten en registros o bancos de datos públicos o privados, conocer la finalidad para los cuales los emplean y, en caso de falsedad o discriminación, para poder exigir la supresión, rectificación, confidencialidad o actualización.

Más tarde, en el año 2000 se sancionó la norma 25.326 de Protección de Datos Personales cuyo fin es el de salvaguardar integralmente los datos de carácter personal que se encontrasen en registros o bancos de datos, garantizando tanto el derecho al honor y a la intimidad de las personas, como el derecho de controlar la

---

<sup>17</sup> BUERES, ALBERTO J. y HIGHTON, ELENA I., "Código Civil y normas complementarias. Análisis doctrinal y Jurisprudencial", Tomo 3 A, editorial Hammurabi, 2005, página 137.

información que sobre las mismas se registre. Esta normativa beneficia con nuevos derechos a los titulares de los datos y exige un estricto código de conducta para la recolección y el tratamiento de los mismos.

### Los límites al Derecho a la Intimidad

Es importante considerar que los derechos no son absolutos, sino que deben ejercerse en armonía con otros derechos, debiendo sujetarse a restricciones razonables.

De acuerdo a Ferreira Rubio<sup>18</sup>, más allá de que el derecho en cuestión puede entrar en conflicto con otros derechos como el derecho a la información o la libertad de prensa, en realidad la protección del derecho a la intimidad se encuentra acotada por factores personales y generales:

1) Las limitaciones de carácter personal son las que se vinculan con características de los sujetos titulares. En este sentido, en el caso de los personajes y figuras de relevancia pública, el umbral de protección es diferente al del resto de los ciudadanos. Al respecto, el

---

<sup>18</sup> BUERES, ALBERTO J. y HIGHTON, ELENA I., "op cit" página 136.

Código Civil comentado de Bueres<sup>19</sup> explica que los personajes no pierden, por el hecho de serlo, el derecho a la vida privada, pero experimentan una reducción del umbral de reserva protegido jurídicamente. Esto implica que hay aspectos de la vida privada de estas personas que, a pesar de pertenecer a esa esfera privada, están librados al conocimiento general. Sin embargo, hay que tener en cuenta que más allá de estas consideraciones, nunca se debe perder de vista que la determinación del umbral de protección requiere en cada caso de la prudente apreciación de los jueces, de acuerdo a las circunstancias.

En el Código anteriormente mencionado, se establece que el fundamento que legitima la intromisión es diferente según el personaje de que se trate:

- si se trata de personas cuyo pensamiento y acción tiene especial trascendencia para el destino de la comunidad (por ejemplo, los dirigentes políticos y los gobernantes), el interés público autoriza a revelar aspectos vinculados con la vida privada, siempre que los mismos tengan alguna trascendencia para la comunidad y su destino;

- si se trata de personas que tienen popularidad aunque su vida no afecte la de los miembros de la comunidad en forma significativa

---

<sup>19</sup> BUERES, ALBERTO J. y HIGHTON, ELENA I., "op cit" página 134.

(por ejemplo, los deportistas o artistas), la intromisión se legitima por la exposición voluntaria del personaje a los requerimientos de la prensa o en la búsqueda de popularidad, lo que los lleva a revelar ellos mismos aspectos de su vida privada;

- si se trata de personajes circunstanciales u ocasionales, los cuales alcanzan notoriedad por verse involucrados en un asunto que atrae la atención del público, se dice que puede llegar a justificarse cierto grado de intromisión en la vida privada, pero sólo en la medida del interés legítimo de la comunidad y en vinculación con el hecho.

Siempre hay que recordar, como se dijo anteriormente, que los límites deberán determinarse en cada caso teniendo en cuenta las circunstancias.

2) Las limitaciones de carácter general provienen de la defensa de intereses superiores, como el bienestar general o el interés público que pueden llevar al Estado, por ejemplo, a solicitar información sobre aspectos vinculados a la salud de las personas, o a su patrimonio o a sus actividades, en el caso de investigación de ilícitos.

En uno u otro caso, tal como sostuvo la Corte Suprema de Justicia de la Nación, será tarea de los jueces armonizar los intereses

en conflicto en cada caso, atendiendo a las circunstancias del mismo y a los valores jurídicos involucrados<sup>20</sup>.

### Derecho al Honor

La propia estima y la fama o reputación que las personas adquieren a medida que transcurre su vida, es una manifestación espiritual humana de suma importancia. Se ha definido al honor de la siguiente manera: “El honor es la propia personalidad entendida como la suma de cualidades físicas, morales, jurídicas, sociales y profesionales, valiosas para la comunidad, atribuibles a las personas”.

El honor puede dividirse en:

a) Honor subjetivo u honra: Se habla de honor subjetivo u honra de la persona cuando el que atribuye las cualidades mencionadas anteriormente es el propio interesado. Al respecto, Soler expresa que “el honor subjetivo puede ser considerado como una autovaloración, es decir, como el aprecio de la propia dignidad, como el juicio que cada cual tiene de sí mismo en cuanto sujeto de relaciones ético sociales”.

---

<sup>20</sup> BUERES, ALBERTO J. y HIGHTON, ELENA I., “op cit” página 136.

b) Honor objetivo u honor propiamente dicho: Se habla de honor objetivo o crédito de la persona cuando los que le atribuyen esas cualidades al interesado son los terceros. Es la fama que una persona obtiene por la estima de los demás, en mérito a sus virtudes o talentos. En este caso, se considera que la persona famosa tiene un área mayor propicia para la ofensa frente a actos que la disminuyen, y por lo tanto es más extendida la posibilidad de lesionarla.

#### Regulación normativa

En el derecho civil, los actos que por dolo o culpa signifiquen ofensas al honor, en principio no pueden ser absueltos por la prueba de la llamada *exceptio veritatis*, o sea, la demostración de la verdad de la culpa atribuida o del defecto difundido. Si bien el artículo 1089 del Código Civil, que se refiere a las denuncias calumniosas, ha hecho la salvedad de que quien cometió la calumnia pruebe la verdad de la imputación, esta norma debe ser interpretada estrictamente, y considerarse que ello sólo es posible si se trata de un delito penal de calumnia.

### Derecho a la Imagen

La imagen es la figura, la fisonomía que la persona tiene, como individuo único e irrepetible.

Así, se ha dicho que el derecho a la propia imagen posee un doble aspecto:

- un aspecto positivo: el derecho que cada persona tiene de captar, reproducir y publicar su propia imagen cómo, dónde y cuándo desee;

- y un aspecto negativo: el derecho subjetivo a la propia imagen es el que la persona tiene de impedir la obtención, adaptación, reproducción y publicación de su propia figura por terceros, sin su consentimiento.

Se ha sostenido que el derecho a la propia imagen confiere al individuo la capacidad de ejercer un control sobre la captación, grabación, uso y difusión de su imagen entendida como representación gráfica de la figura humana, y también de su voz. El derecho a la propia imagen no sólo atiende a los aspectos más concretos y definitorios del mismo, la facultad de consentir en la captación o difusión de imágenes

que reproduzcan la figura humana, sino también a la información que éstas revelan y a su directa relación con las intromisiones en la vida privada. Precisamente se considera que esta relación con la vida privada es la que brinda relevancia constitucional a la protección de la imagen y de la voz.

Lo que preocupa, tal como veremos a continuación, es que las redes sociales constituyen un ámbito en donde se pueden cometer gran cantidad de infracciones sobre el derecho a la imagen.

### Regulación Normativa

El derecho a la imagen está protegido por el artículo 31 de la Ley 11.723 de Propiedad Intelectual y por el Art. 1071 bis del Código Civil.

Al desarrollar lo pertinente a la regulación normativa del derecho a la intimidad, ya se expuso lo dispuesto por el artículo 1071 bis del Código Civil, por lo que ahora específicamente nos referiremos al art. 31 de la Ley 11.723. El mismo establece: “El retrato fotográfico de una persona no puede ser puesto en el comercio sin el



consentimiento expreso de la persona misma, y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarcido daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público.”

Analizando dicho artículo, vemos que el mismo contempla:

- que el retrato fotográfico, es decir, todo medio de captura de imágenes de una persona no se puede dar a difusión pública, sin el consentimiento expreso de la persona misma, y muerta esta, de su cónyuge e hijos o descendientes directos de estos o, en su defecto, del padre o de la madre;

- a su vez, permite que la persona que haya dado su consentimiento pueda revocarlo resarcido daños y perjuicios;

- continúa diciendo que es libre la publicación de retrato cuando se relaciona con fines científicos, didácticos y en general culturales (ésto implica que en el caso de personas célebres se pueden difundir

siempre que estén relacionadas con la actividad del individuo), o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público (esto siempre que la imagen no se saque del contexto del acontecimiento).

De este artículo se ha criticado el requisito del consentimiento expreso, ya que en algunas ocasiones, sea por el silencio o por otros hechos se da el consentimiento tácito, que sería suficiente para disculpar la captación y difusión de la imagen. Sin embargo, de una u otra manera, en estos casos siempre es importante tener en cuenta que cuando el consentimiento se lo presta con un fin determinado no corresponde aprovecharlo para otro.

En cuanto al derecho a la imagen, la jurisprudencia ha dicho que:

- "...La invasión de la esfera reservada del individuo para ser expuesta ante terceros, sin un interés legítimo o un derecho constituido al efecto, configura "per se" la violación a la intimidad. El derecho a la imagen, autónomo y esencial, no es ilimitado, - aunque absoluto por poder ser opuesto "erga omnes" cuando tiene vigencia - sólo cede ante

el interés general de la sociedad, como por ejemplo cuando se relacione con fines científicos, didácticos y en general culturales...<sup>21</sup>;

- "...La violación al derecho a la intimidad y al derecho a la propia imagen surge palmaria e indiscutible con la sola publicación de la fotografía sin el consentimiento expreso de la persona misma ya que nada más se requiere para vulnerar el derecho protegido por el art. 1071 bis del Código Civil y el art. 31 de la ley 11.723<sup>22</sup>.

- "...Sin el consentimiento del damnificado, la mera difusión de la secuencia comporta una intromisión en su vida privada, una lesión a su intimidad y en especial a su imagen que se traduce en un daño moral que debe ser resarcido..."<sup>23</sup>.

En toda situación en que este derecho sea afectado, la medida de la reparación estará dada por la entidad del daño causado que en cada caso deberá ser evaluada por el juez que intervenga en la cuestión.

---

21 Cámara Nacional de Apelaciones en lo Civil, Sala M, "Polino, Marcelo Alejandro c/ Editorial Televisa Argentina S.A. y otro s/ daños y perjuicios", fallo del 07/10/2011, accedido en [www.paradigmadelderecho.com.ar/web/?p=2008](http://www.paradigmadelderecho.com.ar/web/?p=2008), publicado el 03/02/2012.

22 Cámara Nacional de Apelaciones en lo Civil, Sala K, 9-12-99, "Labi, Sergio Juan c/ Editorial Perfil S.A. s/ daños y perjuicios", fallo del 09/12/1999, accedido en <http://ar.vlex.com/vid/labi-sergio-juan-editorial-perfil-perjuicios-35395561>.

23 Cámara Nacional de Apelaciones en lo Civil, Sala B, 14-11-2008, "Resnik, Cristian c/ Ideas del Sur S.A. s/ daños y perjuicios".

En los capítulos que se desarrollarán a continuación, veremos cómo la vertiginosa utilización de las tecnologías de la información por parte de la sociedad de estos días, nos impone coexistir con la idea de que los márgenes de la esfera privada de las personas se han reducido. Esta situación no sólo establece una nueva realidad entre lo público y lo privado, sino que también amenaza el adecuado ejercicio de nuestros derechos a la Intimidad, al Honor y a la Imagen.

### CAPÍTULO III: TRÁFICO DE DATOS PERSONALES

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 de verdaderas **“Redes de Tráfico de datos personales”**.

La problemática que se desprende en torno al **“Tráfico de Datos Personales”** y el modo en que afecta derechos personalísimos

ha de constituir el eje central sobre el que reposa el objeto del presente trabajo. Por tal motivo, brindaremos a continuación algunas nociones conceptuales que entendemos serán de utilidad para su mejor comprensión y análisis de sus implicancias.

El término “*dato*” proviene del latín *datum* (lo que se da) y significa “Antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho”<sup>24</sup>.

Los “datos” en sí mismos, serían representaciones de aspectos de la realidad física, de las ideas, de los sentimientos, de las sensaciones, etcétera, que los integrantes de la especie se traspasan unos a otros, y dado que se utilizan códigos comunes de comunicación, son comprendidos en similar sentido por emisores y receptores<sup>25</sup>.

Más allá de las diferentes concepciones sobre el alcance del término, lo que interesa es que lo “datos” proporcionan “información”, y que la misma merece protección jurídica.

Una “información”, cualquiera sea su tipo o naturaleza, cuando está referida o asociada a una persona (física o de existencia ideal) se

---

<sup>24</sup> Diccionario de la Lengua Española de la Real Academia Española, vigésima segunda edición.

<sup>25</sup> PEYRANO, GUILLERMO, “Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico”, publicado en EL DERECHO- Boletín N° 10.651, 13 de diciembre de 2002.

transforma en un *dato de carácter personal*. Por tanto, los datos personales son una subespecie de los datos en general<sup>26</sup>.

Al respecto, el artículo 2 de la Ley 25.326 de “Protección de Datos Personales y Habeas Data” nos brinda las siguientes nociones conceptuales:

- Datos Personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Datos Sensibles: Datos personales 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.
- Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
- Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de

---

<sup>26</sup> PEYRANO, GUILLERMO, “Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico”, publicado en EL DERECHO- Boletín N° 10.651, 13 de diciembre de 2002.

datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
- Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.
- Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
- Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
- Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

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 datos personales:



- Nombre y apellidos, fecha de nacimiento.
- Número de teléfono, dirección postal y electrónica.
- Datos biométricos (huellas, iris, datos genéticos, imagen, raza, voz, etcétera).
- Datos sanitarios (enfermedades, abortos, cirugía estética, etcétera).
- 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, etcétera.

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. El derecho a la protección de datos personales implica que nadie pueda utilizarlos sin nuestro consentimiento y nos otorga el poder de controlar quién tiene nuestros datos, cómo los ha obtenido, con qué fines y qué uso hará de ellos.

En particular, los denominados “*Datos Sensibles*” 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. Dicha protección busca evitar que estos datos sean utilizados con fines discriminatorios o para generar perjuicios en el supuesto de que se diera a conocer públicamente alguna circunstancia que la persona prefiere mantener en reserva, por ejemplo: el padecimiento de alguna enfermedad.

#### 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. La gente no demostraba interés en conocer hechos ocurridos en lugares lejanos y protagonizados por personas que jamás habían visto, los escasos medios de comunicación favorecían ese desinterés.

Con el advenimiento de las Tecnologías de la Información y la Comunicación (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?

Sin embargo, si analizamos en mayor profundidad este fenómeno, vemos que el desarrollo y expansión de las TICs ha llevado a difuminar el ámbito de lo privado de un modo tal vez no percibido por la mayoría de las personas, sobre todo por aquellas nacidas en este siglo que no vivieron el cambio.

Nosotras, a pesar de nuestra corta edad, logramos percibir los recientes cambios producidos por la masificación de Internet, por un lado en cuanto a la rapidez y bajo costo de las comunicaciones a distancia, sumado a la posibilidad de ver a la otra persona por medio de una cámara web; la frecuente utilización de la Red para obtener información y material de estudio; la facilidad con que se puede almacenar y enviar información por ejemplo por medio del correo

electrónico. Pero por otro lado, llamó nuestra atención la gran cantidad de información personal que arrojan los buscadores al tipiar tan sólo el nombre de determinada persona; la gran exposición de la privacidad propia y ajena que caracteriza a las redes sociales; así como la constante e invasiva publicidad de diversidad de productos y las distintas formas en que las páginas web buscan que nos registremos, desde constituir un requisito para poder utilizar la página hasta la suerte de ganarnos fabulosos premios que “nos serán enviados” si les dejamos nuestros datos personales. Todo ello, nos llevó a investigar el por qué de tanto interés en recabar nuestros datos.

La explicación radica en que “en una sociedad globalizada en donde impera la “Ley del Mercado”, con valores como el “consumismo”, manejar los datos sobre los gustos, los vicios, las posibilidades económicas, el nivel de educación y conocimientos, la salud, las costumbres etc. de miles y miles de personas puede resultar un buen negocio”<sup>27</sup>.

### Los Datos Personales como “mercancía”

---

<sup>27</sup> UICICH, RODOLFO DANIEL, “op cit” página 76. .

Las empresas tienen sumo interés en conocer y manejar los gustos, preferencias, hábitos de consumo de la población, dado que ello les permitirá orientar su producción a las necesidades de consumo, desarrollar publicidad a medida de los consumidores y optimizar el uso de sus recursos en producir aquello que más ventas les garantice. En definitiva, lo que buscan es liderar el mercado con un fin netamente económico, sin importarles cómo llegan a ese objetivo. Es decir, que no las detiene saber que sus prácticas implican intromisiones en la privacidad de los consumidores porque su foco se ubica en incrementar sus ganancias sea como sea.

Además de las empresas fabricantes de productos, existen otros actores sociales que también tienen interés en conocer y manejar 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: enfermedades como 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. Se trata de alguno de los elementos que utilizan las empresas de cobertura médica para excluir a sus clientes.

- ✓ *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<sup>28</sup>.
- ✓ *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<sup>29</sup>.
- ✓ *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.

---

<sup>28</sup> UICICH, RODOLFO DANIEL, "op cit" página 81.

<sup>29</sup> UICICH, RODOLFO DANIEL, "op cit" página 81.

- ✓ *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<sup>30</sup>. 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

---

<sup>30</sup> UICICH, RODOLFO DANIEL, “op cit” página 76.



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 o nos invaden con “cartelitos” para que participemos de los dichos sorteos.

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.

El *correo electrónico (e-mail)* es uno de los servicios de comunicación que ha alcanzado mayor desarrollo en Internet y es un modo eficaz para registrar la identidad de la persona, por esa razón hay que tener especial cuidado a la hora de dar a conocer nuestro e-mail. Existen procedimientos destinados a obtener direcciones de correo electrónico para su uso posterior o para satisfacer intereses específicos de su autor: es el caso de las “cadenas de mensajes” que al ser retransmitidas por los usuarios sin adoptar precauciones (como eliminar las direcciones de los destinatarios), suelen ser recopiladas por programas específicos o por el usuario que ha originado la cadena.

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 mucho más cruel e 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, que merecen una consideración especial, por cuanto son una forma de apropiación de información muy eficaz, a la vez que

desconocida por la mayoría de las personas. Una *cookie* es un archivo de texto, que algunos servidores (equipos que ofrecen servicio a otros equipos de una red al administrar los archivos y las operaciones de red) 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<sup>31</sup>. 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<sup>32</sup>. 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 navegante. Al saber sus preferencias en la web se conoce las preferencias en la vida. Permite ver el histórico

---

<sup>31</sup> UICICH, RODOLFO DANIEL, “op cit” página 81.

<sup>32</sup> UICICH, RODOLFO DANIEL, “op cit” página 82.

de sitios que el usuario ha visitado, los anuncios que ha visto, las transacciones que ha realizado a través de la web. En otras palabras, facilitan la formación del perfil del navegante. Además, es el propio navegante de Internet, cliente del servidor, el que almacena la información que remitirá, sin saberlo, al servidor cuando éste lo requiera<sup>33</sup>.

Si el internauta no adopta ninguna medida de bloqueo las *cookies* se irán almacenando en el directorio respectivo de su disco duro y llegado un momento contendrán información cabal de sus preferencias de navegación.

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. En la práctica ese consentimiento no es solicitado e incluso la mayoría de los usuarios ignoran la existencia de las *cookies*.

Las empresas web que las utilizan deberían ser claras y transparentes con el usuario para que éste acepte o no a la *cookie*. El consentimiento debe reunir ciertas características: ser libre en absoluto, expreso e informado. Por informado entendemos al consentimiento que

---

<sup>33</sup> UICICH, RODOLFO DANIEL, "op cit" página 82.

fue otorgado previo a haber recibido el usuario la totalidad de la información necesaria, pertinente y suficiente para poder decidir.

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 de “informado, ni libre, ni expreso”.

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<sup>34</sup>.

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<sup>35</sup>.

---

<sup>34</sup> UICICH, RODOLFO DANIEL, “op cit” página 85.

<sup>35</sup> AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Recomendaciones dirigidas a usuarios de Internet”, publicado en [www.agpd.es](http://www.agpd.es), accedido a través de:

Al mismo tiempo, la evolución de las tecnologías hace que cada día surjan nuevas formas de captar nuestra imagen personal, antecedentes laborales, transacciones efectuadas, lugares visitados, actividades que realizamos y quien sabe cuántos datos más, 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.

---

[https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/Recomendaciones\\_Internet\\_mayo\\_2006.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/Recomendaciones_Internet_mayo_2006.pdf).

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.

### Las Bases de Datos

La navegación por la Red origina un rastro perfectamente detectable, que se traduce en ciertos datos que sirven para la construcción del perfil del navegante.

Tal como se adelantó al comienzo del presente capítulo, la Ley 25.326 de “Protección de Datos Personales y Habeas Data”, en su artículo 2º nos brinda la siguiente definición:

- Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean

objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

El Diccionario de la Lengua Española de la Real Academia Española define “base de datos” como “Conjunto de datos organizado de tal modo que permita obtener con rapidez diversos tipos de información”.

Años atrás, las bases de datos consistían en ficheros que contenían fichas de papel escritas a mano almacenadas en armarios, estantes, cajones, bibliotecas, etcétera. La utilización de esa información requería de personas que dedicaran tiempo en su búsqueda y el entrecruzamiento de datos resultaba prácticamente imposible. Por tal motivo, la explotación comercial de la información almacenada era al menos, limitada y dificultosa.

Con la irrupción de las Tecnologías de la Información y la Comunicación la situación cambia drásticamente: dando lugar a la captación masiva de datos que son almacenados en ficheros de capacidad y posibilidades de interrelación ilimitadas. 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.

Las bases de datos electrónicas permiten el almacenamiento y 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.

Así es como una impresionante cantidad de información recibida por todos los medios imaginables, con y sin el consentimiento del titular del dato, se guarda en estos almacenes digitales para luego ser “tratada” con los más diversos objetivos<sup>36</sup>. Es muy común que a partir de los datos recogidos, su tratamiento y entrecruzamiento se obtengan nuevos datos, incluso de carácter sensible.

La aparición de nuevas tecnologías como el Data Mining o KDD (knowledge Data Discovery), permiten potenciar la información

---

<sup>36</sup> UICICH, RODOLFO DANIEL, “op cit” página 85.

contenida en las bases de datos por la vía del entrecruzamiento y prospección de los mismos hasta la configuración de los llamados "metadatos". Estos últimos, producto de combinaciones y ensambles de magnitud geométrica, muestran con precisión el perfil exacto de cada persona<sup>37</sup>.

Uno o dos datos personales, o diez datos sobre una persona, resultan inofensivos y no determinativos de la personalidad, pero el entrecruzamiento de los casi trescientos registros digitales que, según se dice, genera un ciudadano hoy en día, por ejemplo en los EE.UU., hacen de la intimidad una verdadera quimera<sup>38</sup>.

Las empresas de publicidad y de marketing directo cruzan, en muchas ocasiones, sus bases de datos personales construidas a partir de los rastros de navegación y la subsiguiente elaboración de perfiles de usuarios, situación que constituye una grave amenaza para nuestra privacidad.

Es evidente que la garantía constitucional argentina de la protección de la intimidad está sumida en una profunda crisis. Las

---

<sup>37</sup> GIULIANO, DIEGO ALBERTO, "El "habeas data" y la explotación de los datos personales: el caso argentino", publicado en CUADERNOS CONSTITUCIONALES DE LA CATEDRA FADRIQUE FURIO CERIAL N° 32. Departamento de Derecho Constitucional y Ciencia Política y de la Administración de la Universidad de Valencia (España), 2000, página 3.

<sup>38</sup> GIULIANO, DIEGO ALBERTO, "op cit" página 3.

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<sup>39</sup>.

Por todo lo expuesto, estamos totalmente convencidas de que el ámbito de privacidad de las personas es cada día más reducido como consecuencia de la invención de tecnologías que son manipuladas por terceros o por empresas que buscan inmiscuirse en dicho ámbito a fin de obtener un beneficio propio.

Por consiguiente, la protección de nuestros datos personales ha adquirido en los últimos años, una trascendencia nunca antes imaginada a fin de preservar nuestra intimidad, privacidad y también seguridad.

Es nuestro deber como ciudadanos luchar por la salvaguarda de nuestros derechos ante la inminencia de un *“florecente mercado”*

---

<sup>39</sup> GIULIANO, DIEGO ALBERTO, “op cit” página 7.

que por el vasto caudal de dinero que genera no parece ser una *“moda pasajera”* sino un negocio que llegó para quedarse.

## CAPÍTULO IV: REDES SOCIALES

Las nuevas tecnologías están introduciendo cambios muy importantes en nuestra sociedad aunque al estar nuestra generación dentro de ellos quizás no podemos ver con perspectiva suficiente la trascendencia que están adquiriendo y tendrán en el futuro. Muchas de estas nuevas tecnologías tienen tal éxito que provocan cambios disruptivos, crean un antes y un después de su existencia<sup>40</sup>.

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 en cuanto a la dimensión sociocultural del ser humano y el calado en la gente común ha afectado a la forma en la que nos relacionamos y el desarrollo de la personalidad. Tanto es así que toda persona ahora tiene al menos dos personalidades e identidades: la real y la digital<sup>41</sup>.

---

<sup>40</sup> CAO AVELLANEDA, JAVIER, Identidad digital y reputación online, la gestión de la e-privacidad, publicado en el sitio web [www.informaticalegal.com.ar](http://www.informaticalegal.com.ar), accedido a través de: <http://www.informaticalegal.com.ar/2012/07/27/identidad-digital-y-reputacion-online-la-gestion-de-la-e-privacidad/>

<sup>41</sup> CAO AVELLANEDA, JAVIER, Identidad digital y reputación online, la gestión de la e-privacidad, publicado en el sitio web [www.informaticalegal.com.ar](http://www.informaticalegal.com.ar), accedido a través de: <http://www.informaticalegal.com.ar/2012/07/27/identidad-digital-y-reputacion-online-la-gestion-de-la-e-privacidad/>

Según ha expresado Fernando Tomeo (Abogado especialista en IP, redes sociales, derecho informático y seguridad de la información): “El nacimiento de las redes sociales ha generado un cambio sustancial en el mundo de las comunicaciones y de las relaciones humanas. Nada será igual. **La web 2.0 es cuna de una revolución sociológica, de la cual no hay regreso**”<sup>42</sup>.

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<sup>43</sup>.

Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como

---

<sup>42</sup> TOMELO, FERNANDO, Striptease digital y datos personales, publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1503463-striptease-digital-y-datos-personales>.

<sup>43</sup> 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: <http://www.gonzalezfrea.com.ar/derecho-informatico/aspectos-legales-redes-sociales-legislacion-normativa-facebook-regulacion-legal-argentina/265/>, página 2.

grupos segmentados: ocio, comunicación, profesionalización, etcétera<sup>44</sup>.

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, sobre todo por la falta de conocimiento reinante en la población acerca de los peligros que ello conlleva.

Dicha situación, se agravó drásticamente a partir de la invención de las redes sociales como Facebook, cuya utilización se ha expandido notoriamente a nivel mundial y cuenta actualmente con, aproximadamente 900 millones de usuarios, por lo que se ha caracterizado como “*La Red Social más popular del planeta*”.

Según la consultora especializada Socialbakers (herramienta para obtener datos estadísticos de las principales plataformas sociales: Facebook, Twitter y LinkedIn) Argentina ha superado los veinte millones de usuarios en Facebook (a octubre de 2012), ocupando el 12º puesto entre los países que más usuarios aportan a la red social y también son los que más tiempo dedican al sitio en el mundo (10,5 horas al mes). Esto quiere decir que casi la mitad de los habitantes de nuestro país tiene un perfil en Facebook, lo cual muestra una velocidad de expansión

---

<sup>44</sup> Estudio sobre la privacidad de datos personales y la seguridad de la información en las redes sociales online. INTECO.

abrumadora si se toma en cuenta que fue recién entre los años 2007 y 2008 que se puso en marcha Facebook en español, impulsando su llegada a los países de Latinoamérica.

Un dato que tal vez haya sido decisivo para su éxito es que cualquier persona con conocimientos informáticos básicos puede tener acceso a la creación y utilización de una cuenta en dicha Red Social.

Sin embargo, esa facilidad de acceso esconde, a nuestro criterio, un lado oscuro y cruel: la falta total de información acerca de su adecuado manejo. Facebook debería garantizar a cada persona que crea una cuenta, un cabal conocimiento de los alcances y posibles consecuencias de su imprudente utilización. Por el contrario, se sirve de un “*Contrato de Adhesión*” para tener por configurado el consentimiento informado de sus usuarios; de ello nos ocuparemos en detalle más adelante.

Podemos afirmar, con total convicción, que Facebook utiliza como “caldo de cultivo” la ausencia de conocimiento acerca de las reales consecuencias que puede acarrear para una persona común la difusión de sus fotografías y publicaciones que contienen datos de carácter personal.



No existe conciencia de que tales datos pueden tener destinos diversos tal como lo explicábamos en el capítulo precedente. En ese orden de ideas, es claro que las redes sociales potencian ciertos peligros en torno a nuestros datos personales: no debe sorprendernos que Facebook tenga a su disposición una mega base de datos digitalizados que puede comercializar con sus anunciantes y demás empresas que se dedican a realizar publicidad a medida de los usuarios.

Al respecto, nos parece oportuno traer a colación un interrogante planteado por el especialista Miguel Sumer Elías: “¿Facebook es gratis? No, no es gratis. La plata no es la única moneda de cambio, se paga con los datos personales”.

También es frecuente la utilización de fotografías, sin el consentimiento de la persona, en la publicidad de servicios, productos y marcas, así como su publicación en diarios, revistas, programas televisivos o mismo su réplica indefinida en la web.

Pero lo peor del caso es la utilización de la red social 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.

Sin intención de realizar un estudio pormenorizado en cuanto al origen, evolución y situación actual de las redes sociales, lo cual excedería el marco del presente trabajo, lo que nos interesa destacar aquí es el modo en que se puede configurar una afectación directa a derechos personalísimos como el Derecho a la Intimidad y a la vida privada, el Derecho al Honor y el Derecho a la Imagen de las personas. Así, cuando un usuario de la Red Social efectúa una publicación puede afectar:

**.- Privacidad personal:** a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento, ya que estas plataformas disponen de potentes herramientas

de intercambio, procesamiento y análisis de la información facilitada por los usuarios.

.- **Privacidad de terceros:** es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata<sup>45</sup>. A su vez, la persona afectada puede iniciar una acción judicial para reclamar los daños y perjuicios que la publicación le hubiera ocasionado.

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 ante los ojos de millones de personas: publicando por ejemplo: su nombre y apellido, fecha de nacimiento, lugar de origen, ciudad actual, lugar de trabajo o estudio, situación sentimental, opiniones religiosas y políticas, preferencias respecto de la música, películas, programas televisivos, deportes, equipos de fútbol, libros, correo electrónico, número de celular y cualquier otro dato que el usuario desee agregar. Aunque parezca

---

<sup>45</sup> GONZALEZ FREA, LEANDRO, “op cit” página 11.

mentira, ello sólo constituye la información básica del perfil de Facebook, que si bien no estamos obligados a brindarla, lo cierto es que la mayoría de los usuarios agrega esos datos al crear la cuenta y los va actualizando con el correr del tiempo. Luego, publican fotografías de su familia, amigos/as, conocidos, de su casa, de las vacaciones de cada verano e invierno, etc.

El problema no son las fotografías en sí mismas, sino la cantidad de información que se brinda con ellas: ubicación y características de la casa; el nombre y actividades de hijos, sobrinos o hermanos menores de edad; eventos familiares tales como nacimientos, cumpleaños, casamientos; las pertenencias materiales, etc. Eso no es todo, también es habitual ver publicaciones en donde se detalla las actividades diarias que se realizan.

Con este relato pormenorizado de las publicaciones que vemos a diario en Facebook queremos dar cuenta del amplio caudal de información que brindan los usuarios diariamente y que permite elaborar una biografía detallada de cada persona; no es casual que el perfil de cada uno sea denominado: “Biografía”.

En tal sentido, Fernando Tomeo expresa: “...Más de 950 millones de usuarios de Facebook y otros tantos de Twitter 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. En muchos casos, este fenómeno de exposición de datos personales es consecuencia del desconocimiento, la imprudencia o el descuido: se utiliza la red social sin la mínima valoración de que se está facilitando al operador de la red uno de los bienes que más cotizan en la actualidad: los datos personales”<sup>46</sup>.

Es fácil verificar que la mayoría de los usuarios no conocen ni analizan las consecuencias que pueden derivarse de sus excesivas publicaciones, porque si lo hicieran no subirían fotografías en las que se brinde tanta información sobre lo que “hacen o tienen” y en las que pueden afectarse derechos personalísimos de terceros, que comprometen su responsabilidad.

En relación a ello, resulta oportuno traer a colación un comentario esgrimido por el especialista antes mencionado: “Las redes sociales tienen poder para definir una posición laboral, la continuidad de un matrimonio, la vigencia de una marca, las ganancias de una

---

<sup>46</sup> TOMELO, FERNANDO, Striptease digital y datos personales, publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1503463-striptease-digital-y-datos-personales>.

compañía y la estabilidad de un gobierno. 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. Sabe Dios en que servidor se termina alojando una foto inapropiada o un comentario poco feliz"<sup>47</sup>.

De allí que a la hora de publicar por ejemplo una fotografía en una red social como Facebook, el usuario debería evaluar si la misma puede afectar el derecho al honor, a la imagen o implique una intromisión en la privacidad de terceros y en caso afirmativo lo correcto y deseable sería que no la publique, dado que si lo hace el afectado tendrá derecho a ser resarcido por los perjuicios que le hubiere ocasionado. La entidad de la reparación estará dada por la magnitud del daño causado, en cada caso.

En efecto, toda persona tiene sobre su imagen y sobre su utilización un derecho exclusivo y su consentimiento es indispensable, no solo a la toma fotográfica sino también a su utilización. Sin el

---

<sup>47</sup> TOMELO, FERNANDO, Etiquetar una foto en Facebook puede afectar derechos personalísimos, publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1441461-etiquetar-una-foto-en-facebook-puede-afectar-derechos-personalisimos>.

consentimiento de una persona, la mera difusión de su imagen importa una intromisión en su vida privada, una lesión a su intimidad que se traduce en un daño moral que debe ser resarcido. Este derecho está protegido por el art. 31 de la ley de propiedad intelectual 11.723 y por el art. 1071 bis del Código Civil. Y este derecho a la imagen está directamente vinculado al derecho a la intimidad y protección de la vida privada que ha sido reconocida como un derecho del hombre por el art. 12 de la Declaración Universal de los Derechos del Hombre y por el art. 17 del Pacto de las Naciones Unidas relativo a los Derechos Civiles y Políticos<sup>48</sup>.

Otro dato a tener en cuenta es que actualmente la *reputación online* forma parte del curriculum de las personas. De hecho, 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

---

<sup>48</sup> TOMELO, FERNANDO, TOMELO, FERNANDO, [Etiquetar una foto en Facebook puede afectar derechos personalísimos](http://www.lanacion.com.ar/1441461-etiquetar-una-foto-en-facebook-puede-afectar-derechos-personalisimos), publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1441461-etiquetar-una-foto-en-facebook-puede-afectar-derechos-personalisimos>.

persona o compañía. La diferencia entre el concepto tradicional y el actual está dada porque, en el presente, hay millones de personas opinando al mismo tiempo y en muchos casos, en tiempo real<sup>49</sup>. Dicha situación, nos conduce a tener que cuidar nuestra reputación online.

En definitiva, la reputación online se ha convertido en un activo más que debe ser “vigilado y gestionado”.

Los efectos de las circunstancias expuestas en el ámbito judicial son variados: formales solicitudes de retiro de contenidos online, revocación del consentimiento informado, demandas de daños contra buscadores y redes sociales por contenidos publicados por terceros, demandas colectivas o "de clase" contra redes sociales por actuar como vehículos de perfiles discriminatorios o violentos, etcétera<sup>50</sup>.

En conclusión, la realidad está demostrando que el striptease de datos personales no sólo puede poner en peligro nuestra seguridad

---

<sup>49</sup> TOMELO, FERNANDO, Etiquetar una foto en Facebook puede afectar derechos personalísimos, publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1441461-etiquetar-una-foto-en-facebook-puede-afectar-derechos-personalissimos>.

<sup>50</sup> TOMELO, FERNANDO, Striptease digital y datos personales, publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1503463-striptease-digital-y-datos-personales>.



personal y familiar sino también nuestro patrimonio cuando se afectan derechos de terceros<sup>51</sup>.

Estamos convencidas de que resulta de vital trascendencia que la sociedad en su totalidad tome conocimiento de que los “**Datos Personales**” se han convertido en un “**activo más**” que cotizan a un alto valor en el mercado y cuya transmisión y comercialización opera preferentemente a través de Internet.

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 aparejada **consecuencias lesivas** para sus propios derechos personalísimos, así como los derechos de terceros.

No debemos olvidar que todo cambio que la sociedad experimenta nos obliga a adaptarnos para poder sobrevivir en ella. En este caso, la Era de la Información nos lleva indefectiblemente a convivir con las TICs a diario y nos coloca ante el desafío de adquirir **habilidades** que nos permitan tener el control sobre ellas, antes de que

---

<sup>51</sup> TOMELO, FERNANDO, Striptease digital y datos personales, publicado en La Nación, accedido a través de la web: <http://www.lanacion.com.ar/1503463-striptease-digital-y-datos-personales>.

otras personas, públicas o privadas, se valgan de ellas para controlarnos.

Asimismo, resulta **ineludible el dictado de una legislación** que aclare las “reglas del juego” para todos los actores de la Red y garantice el debido respeto a los derechos de las personas.

## **CAPÍTULO V: 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 han sido vulnerados mediante la utilización de Internet. El ser humano se ve acosado por la informática y la tecnología, resultando invadido por intromisiones fundadas en razones que las justificarían, aunque no todas ellas sean aceptables.

La realidad se agrava si tomamos en cuenta que es imposible restablecer los derechos anteriormente mencionados, una vez que los mismos han sido atropellados.

Veamos la pluralidad de situaciones y actores que atentan contra los mismos.

### **\* Afectación por el Estado**

En muchas ocasiones, se teme que los Estados recaben información con fines de control y dispongan de datos de la población que puedan ser utilizados para efectuar persecuciones o actos

discriminatorios. Este temor hace que resulte indispensable establecer límites al respecto.

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<sup>52</sup>.

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

---

52 UICICH, Rodolfo Daniel, "La cuestión de la privacidad de los datos en Internet", en La Revista de la Protección de Datos de la Comunidad de Madrid, Nº 30 - 30 noviembre 2007, consultado el 8 de febrero de 2013, accedido el 8 de febrero de 2013 a través de la web <http://www.madrid.org/>.

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 por parte de 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. ¿Pero cómo es esto posible? ¿Cómo se obtienen dichos datos? Veamos.

¿Cuántas veces, mientras navegamos por Internet, nos encontramos con avisos de conocidas empresas que lanzan campañas promocionales en las que se puede ganar un premio? Se nos indica que para poder participar hay que visitar una página de Internet en la que se debe ingresar el número de lote del producto comprado. Una vez en el sitio, resulta que el primer número que se solicita no es el del lote, sino el de nuestro DNI, seguido por nombre y apellido, teléfono,

localidad y provincia. Luego de obtenida toda esa información, ahí sí llega el momento de ingresar ese primer dato solicitado, que termina siendo el último y tal vez el menos importante: el número de lote.

Frente a esta situación, las empresas se defienden diciendo que solicitan datos de las personas que participan en los sorteos que organizan sólo para identificar a la persona en caso de que gane. Lo cierto es que la mayoría de los concursos, sorteos o premios que se ofrecen en Internet, constituyen excusas para obtener datos personales, que no siempre son utilizados con fines comerciales claros. Ésta es una de las tantas formas en que los datos son obtenidos.

Todos estos datos almacenados les permiten a las empresas conocer a su clientela, saber cuáles son sus hábitos de consumo, pudiendo utilizar dicha información para hacer tareas de marketing directo sobre sus clientes. Pero muchas veces, nuestros datos se encuentran, incluso, almacenados en bases de datos de compañías cuyos servicios jamás utilizamos.

Es por eso que se aconseja: no completar formularios al azar ni dar más información que la necesaria, y comprender que brindar información a terceros, nos puede exponer al peligro de que la misma sea utilizada para cometer delitos.

La regulación de dicha situación, llegó en octubre de 2000 cuando se sancionó la ley 25326, que en su primer artículo expone: "La protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas".

A su vez, en el año 2002, se creó el órgano de control de cumplimiento de dicha norma, ante el cual debe ser registrado todo banco de datos: la Dirección Nacional de Protección de Datos Personales (DNPDP), que depende del Ministerio de Justicia. Sin embargo, más allá de la existencia de este órgano de control, lo cierto es que, en la práctica, no todas las bases de datos existentes están registradas. Tampoco ayuda el hecho de que el mencionado organismo sólo ha aplicado escasas sanciones al respecto.

Las bases de datos están formadas por información acumulada sobre las personas, las cuales son legales en caso de que no perjudiquen ni invadan la intimidad de la persona. Así, organismos estatales como ANSES, AFIP o el Registro Nacional de la Propiedad Inmueble poseen una base de datos con información pública sobre las personas, a la cual puede tener acceso cualquier habitante, porque las

mismas no implican vulnerar la intimidad de las personas, ya que dentro de ese ámbito, la información es pública. Además, estos bancos de datos, están regulados por la Ley de Protección de Datos Personales (25.326), la cual establece qué y quiénes podrán obtener información a través de ellos.

Preocupa al respecto del tratamiento de información personal por parte de las compañías y la circulación, cada vez mayor, de bancos de datos por Internet. Para poder proteger nuestra información, es interesante y útil tener en cuenta que, al encontrarse registrado en un banco de datos, mediante el recurso de Habeas Data, cualquiera puede dirigirse a pedir que le informen qué datos tienen sobre él, pudiendo exigir que los modifiquen, actualicen o borren del banco, salvo en el caso de las excepciones que establece la ley como ocurre con AFIP, de los que no se puede pedir la baja.

Lo que resulta verdaderamente alarmante es la existencia de un mercado de datos personales. Existen empresas que se dedican exclusivamente a la venta de datos personales por Internet, las cuales otorgan información de las personas como un servicio, a través del pago de 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.

Lo peligroso es el tipo de información que manejan y la imposibilidad de comprobar de qué manera esos datos son obtenidos.

Respecto a este tipo de empresas, 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<sup>53</sup>.

Así es como llegamos a la conclusión de que impedir la indebida intromisión de las grandes empresas parece una tarea difícil, pero se hace indispensable hacer cumplir la ley y poner un freno a la manipulación de datos personales que están llevando a cabo a través de la utilización de Internet.

---

53 ARIAS, MARÍA CLARA, "¿Legal o ilegal? cómo funciona la venta de datos personales en Internet", 27 de julio de 2012, en la Página 24 Conurbano, consultado el 7 de marzo de 2013, accedido el 7 de marzo de 2013 a través de <http://24con.infonews.com/conurbano/nota/56632-legal-o-ilegal-como-funciona-la-venta-de-datos-personales-en-internet/>

\* Afectación por parte de los Particulares a través de las Redes Sociales

Si bien en el capítulo que antecede abordamos la problemática que suscita la difusión de imágenes perpetrada a través de la utilización de las redes sociales, en esta oportunidad nos detendremos a analizar el peculiar modo en que afecta los derechos de las personas.

Lo publicado en redes sociales puede afectarnos en lo cotidiano. Desde quedar expuestos a delitos, en caso de publicar información personal detallada hasta pasar por divorcios o despidos laborales, si las fotos o videos subidos no son considerados correctos o adecuados por quien los mira.

Debemos preservarnos de la forma en que las nuevas tecnologías utilizan nuestros datos para evitar la lesión a nuestros derechos fundamentales, y para lograrlo, se puede seguir las reglas que propone Javier Cao Avellaneda<sup>54</sup>.

---

54 CAO AVELLANEDA, Javier, "Identidad digital y reputación online, la gestión de la e-privacidad", 27 de julio de 2012, en su blog personal "Apuntes de Seguridad de la Información" (Ingeniero en Informática, Consultor en seguridad de la información, CISA y Auditor ISO 27001), consultado el 8 de febrero de 2013, accedido el 8 de febrero de 2013, a través de la web <http://seguridad-de-la-informacion.blogspot.com.ar/2012/07/identidad-digital-y-reputacion-online.html>.

- Utilizar el sentido común y tener siempre presente que aquello que se sube, una vez publicado no podrá ser controlable, porque aunque se borre, muchas veces ya existen copias locales que hacen que el contenido se perpetúe.

- Si se controla la intimidad propia, no exponamos la de los demás, ni la de familiares ni la de conocidos.

- No exponerse más de lo deseado.

- Ayudarse con los servicios de alertas de Google que permiten vigilar tu nombre. Así, si bien es difícil controlar lo que otros publican sobre uno mismo, es posible monitorizar de forma pasiva lo que aparece.

- Contar con el respaldo de servicios profesionales que sepan canalizar tus problemas por las vías jurídicas más adecuadas para que tus derechos de protección de datos o de defensa del honor o intimidad sean respetados, incluso en Internet.

Otra de las cuestiones de la que vale la pena hacer mención, es lo que sucede con la violación, en concreto, del derecho a la imagen y las consecuencias nefastas que la misma trae aparejada en relación a los restantes derechos, como la intimidad y el honor.

"En los últimos tiempos, la expansión de la tecnología alcanza tal nivel que es común que cualquier situación de la vida cotidiana, por poca espectacularidad que tenga, igual se vuelve fotografiable o filmable. Y señala que muchas veces este nuevo uso de las fotos y filmaciones en la red deriva en demandas judiciales"<sup>55</sup>.

Contamos entonces con protección legal que impide que cualquier persona capture o difunda la imagen de otra sin su previo consentimiento: en caso de que esa imagen sea reproducida, esa persona tiene derecho a solicitar a la justicia que ordene el cese de la divulgación de su imagen, pudiendo también pedir el resarcimiento económico que estime adecuado, tal como lo anticipamos en el capítulo IV.

El derecho a la propia imagen implica el derecho de cada persona de captar, reproducir y publicar su propia imagen cómo, dónde y cuándo desee, y a su vez, el derecho que cada persona tiene de impedir la obtención, adaptación, reproducción y publicación de su propia figura por terceros, sin su consentimiento.

Ya hace tiempo que encontramos violaciones al derecho a la

---

55 MEYER, GRACIANA, "Entrevista al abogado Miguel Sumer Elías, especialista en Derecho Informático", 14 de diciembre de 2012, consultado el 7 de marzo de 2013, accedido el 7 de marzo de 2013, a través de la web "[www.informaticalegal.com](http://www.informaticalegal.com)".

imagen, acorde con las tecnologías vigentes en cada época, pero también de acuerdo a quién es la persona que captura la imagen.

Basta recordar el emblemático caso "Ponzetti de Balbín". Encontrándose el doctor Ricardo Balbín internado de gravedad en una clínica de la ciudad de La Plata, un fotógrafo sin autorización tomó una fotografía del paciente en dicho estado, la cual fue publicada por la revista "Gente y la actualidad" en septiembre de 1981. Esta publicación provocó el sufrimiento la familia del Dr. Balbín y como consecuencia, su esposa y su hijo promovieron una demanda por indemnización por daños y perjuicios contra "Editorial Atlántida S.A." propietaria de la revista, por violación del derecho a la intimidad, determinándose que las fotografías no eran necesarias para informar sobre el estado del Dr. Balbín<sup>56</sup>.

Lo que sucede es que en el caso anteriormente mencionado, la violación al derecho a la intimidad y a la imagen venía determinada por la publicación en una revista de una fotografía capturada por un fotógrafo. En la actualidad, es común que sean las mismas personas afectadas las que toman sus fotografías o filman videos íntimos, los

---

56 "Ponzetti de Balbín, Indalia c. Editorial Atlántida, S.A. s/ daños y perjuicios", fallo del 11/12/1984, accedido en [notasfallosconstitucionaluba.blogspot.com.ar](http://notasfallosconstitucionaluba.blogspot.com.ar)

cuales son subidos a la red por desconocidos. Ahora es Internet el medio utilizado para propiciar el daño y transgredir los derechos.

Son múltiples los casos en que fotografías o videos íntimos de personas del mundo del espectáculo, que en principio estaban alojados en computadoras o celulares de éstos últimos, son apropiados por individuos que luego difunden dicho contenido privado en Internet. Así, dichas imágenes circulan por la web mortificando la vida de sus protagonistas.

Pero no es necesario ser famoso para ser víctima de dicha problemática: cualquiera puede verse afectado diariamente. Al respecto, el abogado Miguel Sumer Elías detalla situaciones que ponen en riesgo nuestra imagen e intimidad sobre todo entre los más jóvenes, lo cual no implica que a los adultos no les pase.

El experto menciona prácticas adolescentes como el "sex teen", consistente en sacarse fotos provocativas y pasarlas por teléfono, o el "despecho online", que tiene lugar cuando se vuelca en la web la bronca de las parejas que se pelean, publicando imágenes íntimas. Las consecuencias son tremendas porque pueden ir desde la lógica humillación de quedar expuestos ante los ojos de todos hasta terminar siendo vinculado a un sitio pornográfico.

Famosos o no, todos los casos actuales tienen algo en común: la vulneración de su intimidad mediante una ilegítima intromisión en sus vidas privadas, viralizando el daño a su imagen y reputación. Los derechos a la intimidad, al honor y a la imagen son puestos en jaque.

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.

#### \* 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. En Argentina, se pueden citar como los más usados a Google, Yahoo! y Microsoft Live Search.

Sin embargo, en muchas ocasiones, los buscadores de Internet retienen grandes volúmenes de datos de sus usuarios. Lo cuestionable es que éstos últimos no son conscientes ni cuentan con la información necesaria sobre el manejo de sus datos personales, ya que incluso lo

explicado al respecto en las políticas de privacidad de los servicios de búsqueda puede no ser comprendido por las personas que utilizan Internet.

Más allá de lo prácticos y provechosos que resultan para obtener información, ya sea con fines educativos o laborales, 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.

Numerosas 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 los buscadores de Internet antes mencionados para que los mismos eliminen los contenidos agraviantes, aunque no todas corrieron con la misma suerte.

Veamos las distintas soluciones adoptadas por los tribunales en cada caso respecto a la filtración de contenidos injuriosos por parte de los buscadores en cuestión y qué sostienen respecto a la colisión de la medida con el derecho a la información.

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, y que el argumento de que los buscadores realizan las búsquedas mediante el uso de robots que actúan en forma automática no es relevante por cuanto el código utilizado para desarrollar estas tareas es diseñado y desarrollado por humanos.

Esta fue la posición adoptada en septiembre de 2012 por la Cámara Civil que condenó a los buscadores Google y Yahoo! a pagar daños y perjuicios a la actriz Paola Krum por uso no autorizado de su imagen en los resultados de búsqueda. La sentencia ordenó a los buscadores a eliminar en forma definitiva de sus respectivas páginas de resultados de búsqueda la imagen y/o el nombre de la actriz vinculados con sitios web de contenido sexual, erótico y pornográfico, de oferta de sexo y similares, con la única excepción de aquellos sitios que

correspondieran a ediciones digitales de medios de prensa<sup>57</sup>.

Analizando esta postura, y ya vinculándola con la posible colisión de lo solicitado por quien demanda con el derecho a la información, en el caso anteriormente mencionado, la Cámara sostuvo que “las medidas requeridas por la accionante no persiguen evitar una crítica, ni vedar la difusión de un pensamiento o una idea, ni silenciar algún tema relacionado con el interés público” sino “la defensa de valores particularmente protegidos por el ordenamiento jurídico nacional e internacional, impidiendo la propagación de la actividad ilícita de quienes utilizan su nombre y/o imagen para publicitar engañosamente sitios vinculados con el comercio sexual o la pornografía”.

Los jueces indicaron que “ninguna de las peticiones realizadas por la accionante violenta el derecho a la información, ni de quienes resulten ser los propietarios de los diversos sitios que introdujeron ilícitamente su nombre o imagen, ni de los buscadores en tanto que reproductores en sus propios sitios y que no hay nada que pueda ser calificado de noticia ni de opinión, por lo que no cabe tampoco hablar de censura”.

---

<sup>57</sup> Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, Sala J. “Krum, Andrea Paola c/ Yahoo de Argentina S. R. L y otros/daños y perjuicios”, Expte. N° 84/103/2007, fallo del 31/08/2012, accedido en <http://www.paradigmadelderecho.com.ar/web/?p=4285>

- 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. Por ello, y hasta que no exista una legislación al respecto en Argentina, 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. del Código Civil . Constituye ejemplo de esta postura lo expuesto en la causa "Da Cunha Virginia c. Yahoo de Argentina SRL y otro s/ daños y perjuicios", de agosto de 2010<sup>58</sup>.

La vinculación de esta postura con el derecho a la información, hace que los jueces consideren que la eliminación indiscriminada de sitios web de los buscadores "comporta una inevitable afectación del acceso a la información por cuanto significa poner en un plano de igualdad los sitios de contenidos lícitos, los sitios de noticias y de información de interés público". En ese sentido, destacan que la Ley 26.032 dispone que "la búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, está amparada

---

58 Cámara Nacional de Apelaciones en lo Civil, Sala D, "Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y Perjuicios", Expte. Nº 99.620/2006, fallo de agosto de 2010, accedido en [www.hfernandezdelpech.com.ar/](http://www.hfernandezdelpech.com.ar/)

por la garantía constitucional de la libertad de expresión”.

En algunos casos, los jueces sostienen que sólo puede existir culpa desde el momento que el buscador tenga conocimiento efectivo de la infracción, mediante una notificación judicial.

“Si el Buscador no fue notificado de la existencia del contenido ilegal, no es responsable por los resultados de búsqueda que ofrece. Precisamente, los buscadores argumentan en su defensa, que no son un medio sino un indexador, por lo cual no pueden bloquear contenidos, salvo que se les provean las URL (Localizador de Recursos Uniforme), con un fallo judicial que avale el bloqueo. Pero si el buscador fue notificado extrajudicialmente y se le reclamó su bloqueo, debe realizar las tareas necesarias para dejar sin efecto el vínculo o bloquear su contenido”<sup>59</sup>.

En caso de haber sido notificado y no proceder a realizar el bloqueo requerido, la conducta antijurídica consiste en "la omisión de eliminar de su listado de resultados las páginas de contenidos violatorios de derechos una vez que son notificados de su carácter

---

59 TORNABENE, Inés, "Buscadores de Internet: ¿están o no obligados a filtrar contenidos injuriosos?", en HABEAS DATA Revista Electrónica del Centro de Protección de Datos Personales, 11 de diciembre de 2012, consultado el 7 de marzo de 2013, accedido el 7 de marzo de 2013, a través de la web <http://habeasdatacpdp.wordpress.com/tag/fallos-judiciales/>

ilícito”. Así fue como la sentencia de la Cámara Civil y Comercial Federal dispuso que el buscador Yahoo! debía pagar determinada suma de dinero a la modelo Priscilla Prete en concepto de resarcimiento por daños al no ocuparse de atender a la solicitud de eliminar los contenidos agraviantes, luego de notificado. Aquí, los jueces expusieron que no es obligación de los buscadores chequear contenidos “a fin de ejercer un filtrado previo”, pero esto no los excusa por la omisión de eliminarlos una vez puesto en aviso por el afectado<sup>60</sup>.

Por otro lado, a veces surge el hecho de un perjuicio a los propios demandados por lo que debe haber una responsabilidad compartida entre las partes a la hora de accionar. “Debe requerirse del damnificado un obrar leal y de buena fe, debiendo identificar en forma concreta el contenido cuyo bloqueo solicita y su ubicación, y fundamentos”. Así, encontramos el planteo de Pamela David contra la empresa Microsoft Argentina y Bing, su buscador de Internet: en primera instancia se ordenó a la compañía que adoptara “las medidas necesarias para eliminar toda referencia que permita identificar y

---

60 Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala I, “Prete Priscila c/ Yahoo de Argentina S.R.L. s/ daños y perjuicios”, Causa N° 9847/2007, fallo del 06/09/2012, accedido en <http://www.paradigmadelderecho.com.ar/web/?p=5111>, publicado el 21/09/2012.

vincular su nombre a través del buscador a sitios de "contenido sexual, pornográfico, venta de sexo o de elementos sexuales o cualquier otra actividad sexual". Sin embargo, Microsoft pidió que fuera la afectada quien indicara qué sitios herían su sensibilidad "a fin de poder cumplir con la medida cautelar decretada". Entonces, la Sala Tercera de la Cámara en lo Civil y Comercial Federal resolvió que la modelo deberá presentar "copia del contenido del o los sitios en particular, de modo tal que se pueda valorar si se produce afectación de sus derechos personalísimos, siendo necesario que sea David quien individualice cuáles son los resultados que considera lesivos<sup>61</sup>.

Como podemos apreciar, 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 opiniones, criterios e interpretaciones que no son idénticos, sino muchas veces contradictorias, porque dependen de la postura que cada juez tenga sobre la materia.

Teniendo en cuenta que los buscadores de Internet son utilizados en el mundo entero, lo ideal en este aspecto sería fijar reglas

---

61 Cámara en lo Civil y Comercial Federal, Sala Tercera de la Cámara en lo Civil y Comercial Federal, "Pamela David Gutiérrez c/ Microsoft de Argentina SA y su buscador de Internet, Bing".

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.

De lo expuesto, podemos sostener que los derechos a la intimidad, al honor y a la imagen personal han variado intensamente como consecuencia de la revolución tecnológica. Esta circunstancia, sumada a la falta de formación de los usuarios sobre el uso correcto de estas nuevas tecnologías, nos lleva a la necesidad de ampliar el ámbito de protección de los derechos que constituyen el objeto del presente trabajo, y establecer nuevos instrumentos de tutela jurídica.

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 ajenos.

Cuando se habla de Internet y su regulación, se recurre a la frase "no es posible ponerle puertas al campo". Sin embargo, en algunos supuestos al menos habría que establecer límites infranqueables: "Internet no tiene forma y no entiende de territorios,

pero jamás debería poder avasallar a la Justicia"<sup>62</sup>.

---

62 CAO AVELLANEDA, Javier, "¿Puede Internet avasallar a la Justicia?", 12 de junio de 2010, en su blog personal "Apuntes de Seguridad de la Información" (Ingeniero en Informática, Consultor en seguridad de la información, CISA y Auditor ISO 27001), consultado el 8 de febrero de 2013, accedido el 8 de febrero de 2013, a través de la web <http://seguridad-de-la-informacion.blogspot.com.ar/2012/07/identidad-digital-y-reputacion-online.html>.



## CAPÍTULO VI: PROTECCIÓN DE DATOS PERSONALES

En la Sociedad de la Información, los datos personales se han convertido en una *poderosa mercancía* que cotiza a un alto valor en el mercado, dando origen a un *incipiente y acaudalado negocio* en torno a ellos: **“El Tráfico de Datos Personales”**.

Consecuentemente, hoy vivimos en una especie de Panóptico de Foucault, en donde la monstruosa recolección de información y el inmenso tráfico de datos personales constituyen una amenaza constante para nuestras libertades y derechos personalísimos, impactando fundamentalmente sobre el Derecho a la Intimidad.

Se trata básicamente del producto de otro fenómeno: el crecimiento y expansión de Internet a nivel mundial y la cotidianeidad de su utilización por millones de personas en tiempo real que ha facilitado la reproducción y transmisión de contenidos, al punto de concretarse prácticamente al instante.

Asimismo, un factor decisivo en la explosión de tal negocio ha sido la creciente demanda de información confidencial que es utilizada y

manipulada para los más diversos propósitos, junto con la proliferación de una ingente variedad de tecnologías puestas a su servicio.

Creemos firmemente, que esta marea de alteraciones 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 perpetradas a través de Internet. Ante tal desafío, se enfrenta la comunidad internacional en nuestros días, como corolario de la dimensión global que caracteriza a la Red de Redes.

### La “Aldea Global”

Como es sabido, Internet ha permitido la comunicación e interacción de millones de personas a nivel mundial, situación que nos lleva a hablar de la conformación de una “*gran aldea global*”, en donde la información es transmitida y retransmitida, vulnerando los clásicos límites territoriales entre los distintos Estados.

La realidad de Internet es plurilocal y diluyente de la frontera geográfica y de la autoridad controladora. La frontera como pauta de referencia de la regulación pierde gran parte de su sentido y la base virtual sobre la que se asienta Internet mengua en grado sumo la fuerza de la medida espacial física. El mantenimiento por parte del Estado de todo su poder en el interior de su territorio no es suficiente para asegurar el dominio de la Red<sup>63</sup>.

Es fácil advertir que los Estados están experimentando serias dificultades a la hora de controlar este fenómeno. El salto de los límites estatales que se produce en Internet dificulta la persecución por parte de las autoridades nacionales de las infracciones referidas a la captura, tratamiento y transmisión de datos personales sin el consentimiento de sus titulares.

En definitiva, la expansión de Internet trajo consigo un riesgo adicional en lo que respecta a la protección de datos personales y la preservación de la intimidad de los usuarios.

Por consiguiente, la salvaguarda de los derechos fundamentales de las personas ante este fenómeno no solo reclama de normas protectoras a nivel nacional sino que exige, a nuestro humilde

---

<sup>63</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, "op cit" página 142.

entender, una tarea conjunta y coordinada de toda la comunidad internacional.

### Aproximación conceptual y principios rectores

El advenimiento de la era informática provocó un notorio agravamiento de la potencialidad dañosa que deriva del “tratamiento de datos de carácter personal”.

Esta situación hizo que se empezara a debatir acerca del “*derecho a la protección de datos*” o también denominado: “*derecho a la autodeterminación informativa*”; “*libertad informática*”; “*intimidad informática*”; etcétera. Son distintas rotulaciones utilizadas por la doctrina que coinciden en sus contenidos esenciales.

Hondius refiere a la “*protección de datos*” 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”<sup>64</sup>.

---

<sup>64</sup> HONDIUS F., “A decade of international Data Protection”, *Netherlands of International Law Review*, vol 30, nº 2, 1983, página 105.

Puccinelli sostiene que el “derecho a la protección de datos” refleja “la facultad con que cuenta toda persona para actuar per se y para exigir la actuación del Estado a fin de tutelar los diversos derechos que pudieran verse afectados en virtud del tratamiento de los datos de carácter personal que les conciernen”<sup>65</sup>.

Con la denominación “*libertad informática*”, Pérez Luño alude a un nuevo derecho fundamental, propio de la tercera generación, que tiene por finalidad “garantizar la facultad de las personas de conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos; controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión”. A su vez, según el citado jurista, la protección de datos personales tutelaría “el conjunto de bienes o intereses que puedan ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables”<sup>66</sup>.

Entendemos que, en definitiva, el derecho a la protección de datos no es sino “la suma de principios, derechos y garantías

---

<sup>65</sup> 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, pág. 122.

<sup>66</sup> PÉREZ LUÑO, ANTONIO E., “Los derechos humanos en la sociedad tecnológica”, en Mario Losano y otros, “Libertad informática y leyes de protección de datos personales”, CEC, Madrid, 1989, página 140.

establecidas en favor de las personas que pudieran verse perjudicadas por el tratamiento de datos de carácter personal a ellas referidos”.

Al decir de Puccinelli, 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, y que se pretende con su creación brindar una tutela especial a las personas -físicas y jurídicas- frente a las afecciones a los derechos fundamentales que pudieran sufrir éstas a partir del tratamiento de datos. Entre tales bienes jurídicos están implicados tanto principios rectores de los derechos humanos: libertad, dignidad e igualdad, como múltiples derechos fundamentales: intimidad, identidad, honor, propiedad sobre los datos, etcétera<sup>67</sup>.

Al respecto, resulta clarificador lo señalado por Bidart Campos, cuando sostuvo: “Dentro del ámbito tutelar de los derechos personales, y en afinidad con las garantías clásicas frente al Estado, hay “derechos” denominados tales que, en rigor, sirven y se usan para la defensa de otros derechos; a aquellos denominados derechos que se dirigen a

---

<sup>67</sup> PUCCINELLI, OSCAR RAÚL, “op cit” página 125.

proteger otros derechos se les asigna la categoría y naturaleza de *garantías*<sup>68</sup>.

Puccinelli plantea cuatro interrogantes en atención a la protección de datos personales que nos resultaron lo suficientemente explicativos, motivo por el cual los traemos a colación en el presente trabajo:

- ✓ *¿Qué se protege?* Los datos de carácter personal, que son los referidos a personas identificadas o identificables, pero únicamente como medio para tutelar los bienes jurídicos que el uso de esos datos puede vulnerar.
- ✓ *¿De qué se protege?* De ciertas actividades respecto de tales datos, conocidas técnicamente como “tratamiento” y dentro de las cuales se encuentran, entre muchas otras, las operaciones de acceso, registración, elaboración y transferencia a terceros.
- ✓ *¿De quién se protege?* De cualquiera que realice el tratamiento de datos de carácter personal, cuando ese tratamiento exceda o pueda razonablemente exceder de uso estrictamente privado y personal de quien lo realiza.

---

<sup>68</sup> BIDART CAMPOS, GERMÁN J., “Repensando las garantías constitucionales”, “L.L”, 1991-B-977/8.

✓ *¿Cómo se protege?* El derecho a la protección de datos puede ser tutelado de diversas formas, de las cuales las más comunes son:

1. Las normas generales o específicas, convencionales, constitucionales o legales que establezcan:
  - a. Ciertas reglas mínimas para el tratamiento de datos de carácter personal y para la habilitación de las bases y bancos de datos, específicamente limitando sus actividades a las estrictamente necesarias para la finalidad para la que son autorizadas.
  - b. Derechos de los registrados.
  - c. Sanciones administrativas y penales para quienes infrinjan las normas.
  - d. Mecanismos institucionales de garantía (como un órgano de control).
  - e. Recursos ante ese órgano de control y otras vías administrativas idóneas.
  - f. Vías judiciales de amparo específicamente amoldadas a la tutela de los datos; por ejemplo: el hábeas data del constitucionalismo iberoamericano.



2. Los contratos respecto del tratamiento de determinados datos.
3. Los códigos de conducta, deontológicos o de ética.
4. Los instrumentos internacionales (globales o regionales) que regulen ciertos aspectos comunes, en especial lo relativo al flujo de datos transfronterizos<sup>69</sup>.

En la actualidad hay una tendencia a la homogenización de principios y criterios a nivel internacional en lo que respecta a la protección de datos personales. En particular citaremos a continuación los principios básicos fijados en la “Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal”, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid:

✓ Principio de lealtad y legalidad:

1. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto

---

<sup>69</sup> PUCCINELLI, OSCAR RAÚL, “op cit” página 127.

en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

2. En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados.

✓ Principio de finalidad:

1. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable.

2. La persona responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.

✓ Principio de proporcionalidad:

1. El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas en el apartado anterior.

2. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.

✓ Principio de calidad:

1. La persona responsable deberá asegurar en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados.

2. La persona responsable deberá limitar el periodo de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos.

✓ Principio de Transparencia:

1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.

2. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende

realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

3. Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.

4. Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.

5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones

establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

✓ Principio de Responsabilidad: La persona responsable deberá:

- a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y
- b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias.

A tales principios básicos podríamos adicionar otros tres principios que han sido consagrados por normas europeas de protección de datos personales, a saber:

- ✓ Limitación de la recolección: estatuye que los datos deben ser obtenidos por medios lícitos, es decir, con el conocimiento y consentimiento del sujeto de los datos o con autorización legal, y limitarse al mínimo necesario para alcanzar el fin perseguido por la recolección.

- ✓ Confidencialidad: conforme al cual el acceso de terceros a los datos debe tener lugar con el consentimiento del sujeto o con autorización legal.
- ✓ Salvaguarda de la seguridad: por el cual el responsable del registro de datos personales debe adoptar medidas adecuadas para protegerlos contra posibles pérdidas, destrucciones o acceso no autorizado.

El tratamiento de datos personales con fines comerciales debe acatar a rajatabla todos y cada uno de los principios enumerados precedentemente, fundamentalmente debe exigir siempre el consentimiento previo del afectado, sea cual fuere el país en el que se esté llevando a cabo. No obstante, Internet facilita un escenario en el que se producen constantes transgresiones a estos principios, vulnerando en definitiva, los derechos personalísimos de los individuos.

Un claro ejemplo de ello se presenta en la acumulación de datos sobre la navegación sin que medie un consentimiento inequívoco del navegante. Particular relieve cobran, en este sentido, las ya aludidas cookies, que entran en la computadora sin consentimiento del usuario y, de haberlo, con una información que se limita a la simple recepción de la cookie y no acerca del tratamiento de los datos que

contiene<sup>70</sup>. Tampoco se informan las finalidades que persigue el responsable de la base de datos, ni su identidad, ni los destinatarios en caso de cesión de datos, ni conocemos cuál es el período de conservación de nuestros datos, ni cuántas personas o empresas pueden llegar a tener acceso a los mismos. Además, si la cookie recoge el nombre del navegante, cuando éste ha personalizado su navegador, se convierte en un dato personal.

En la misma línea de inadmisibilidad se sitúa la ya vista elaboración de perfiles del navegante y la habitual cesión de datos que se opera en la Red de unas empresas a otras, sin que exista consentimiento inequívoco del afectado.

Ahora bien, es cierto que aún existen violaciones a los principios mencionados sobre todo por parte de los monstruos de la Red como son las multinacionales Facebook o Google, de cuyas políticas de privacidad nos ocuparemos en detalle más adelante. Pese a ello, creemos que la elaboración de estándares internacionales sobre protección de datos personales en relación a las técnicas de tratamiento podría significar el primer paso en la toma de conciencia de la trascendencia de la problemática a nivel internacional y en la futura

---

<sup>70</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, "op cit" página 137.

redacción de un documento internacionalmente vinculante que “contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado”<sup>71</sup>.

### Regulación Normativa en el Derecho Comparado

Nos parece oportuno en esta parte del trabajo, hacer mención a los diferentes cuerpos normativos que regulan el tratamiento informatizado de los datos de carácter personal, a efectos de exaltar, entre otros aspectos, por un lado, la labor que viene cumpliendo el Parlamento Europeo y el Consejo de la Unión Europea por puntualizar y establecer un marco de garantías y medidas de protección a los derechos involucrados en dicho tratamiento (con mayor énfasis en el derecho a la intimidad y subsidiariamente de la información, la expresión, el honor y la imagen, entre otros); y por otro, el marcado

---

<sup>71</sup> Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid. Labor conjunta de los garantes de la privacidad de casi cincuenta países, bajo coordinación de la Agencia Española de Protección de Datos, accedido a través del sitio web: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31\\_conferencia\\_internacional/estandares\\_resolucion\\_madrid\\_es.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf)



contraste que existe en el modo de regular la problemática al otro lado del océano: Estados Unidos.

Respecto de las leyes de protección de datos personales es posible clasificarlas en *cuatro generaciones*, según sus contenidos y evolución en la regulación del fenómeno informático en entronque con el derecho.

En la **primera generación** de estas leyes se hallan las denominadas *leyes pioneras* en la regulación y tratamiento (informatizado o no) de datos de carácter personal: La *Ley Federal alemana de protección de datos personales* y Ley Sueca “*Data Lag*” de 11 de mayo de 1973. Según Mirabelli, estas leyes son tendencialmente restrictivas puesto que se sujetan al requisito de “la autorización previa” para la creación de los “ficheros” o bancos de datos, limitando excesivamente la recolección de los “datos sensibles” e instituyendo organismos con funciones y estructura cuasi jurisdiccional para la concesión y el ejercicio del control de los mencionados banco de datos<sup>72</sup>.

---

<sup>72</sup> MIRABELLI, “Banche dati e contemperamento degli interessi”, *Banche dati telematica e diritti della persona*, Cedam, Padova, 1984, pág. 160.

En una **segunda generación** de leyes protectoras de los datos personales se destacan la de Francia en 1974; Privacy Act estadounidense de 1974; Noruega en 1978; Luxemburgo en 1981, etcétera. Las leyes en esta etapa se caracterizan por el sistema de “la notificación”; se introduce la figura del responsable del fichero o banco de datos, se ingresa en la técnica legislativa de la conceptualización de los términos técnico cerrados y abiertos utilizados en las nuevas tecnologías de la información y la comunicación (TIC) que inciden en el derecho y se instituye, a partir de éstas, los denominados “principios fundamentales de la protección de datos”.

En paralelo y con idénticos propósitos, surgen normas de ámbito internacional europeo sobre el tratamiento informatizado de datos: La **Recomendación del Consejo de la OCDE** de Septiembre 30 de 1980, por la que se formulan “directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales” y **El Convenio Europeo de Estrasburgo** de 28 de Enero de 1981”, relativo a la “protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”.

En la “**tercera generación**”, se ubican las normas jurídicas nacidas en la década de los noventa. En esta se ubican la “*La ley*

*española de regulación del tratamiento automatizado de datos de carácter personal*”, de 29 de Octubre de 1992, conocida también como LORTAD, reformada en 1999, por la “*Ley Orgánica de Protección de Datos*” o LOPD, Ley 15 de 1999; como también la “*Privacy and data Protection Bill 1994 (NSW)*” o *Ley de protección de la intimidad y los datos personales en Australia*. Esta generación de leyes se caracteriza según Orti Vallejo, siguiendo a *Pérez Luño*, por ser más “liberalizantes del uso de ficheros de datos personales” y establecer un amplio marco de principios, derechos y obligaciones para las personas naturales, jurídicas, públicas y privadas<sup>73</sup>.

Una **cuarta generación** de normas surge con la expedición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, “*relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*”. Esta generación se caracteriza por plantear como epicentro el principio-derecho de la libre circulación de datos personales entre los países miembros de la Unión Europea e incluso entre países terceros, previo cumplimiento de requisitos sine qua nom; la consagración de principios, derechos (como el de información y de

---

<sup>73</sup> ORTI VALLEJO, A, “Derecho a la intimidad e informática”, Ed. Comares, Peligros (Granada), 1994.

Hábeas data) y obligaciones en todas las fases, etapas o ciclos informáticos del procedimiento informatizado de datos, cuando se realiza con soportes, medios y aplicaciones informáticas electrónicas y telemáticas y la plasmación del llamado **derecho de oposición** al tratamiento informatizado de datos personales, como un derecho personalísimo de los titulares de los datos personales<sup>74</sup>.

En términos generales, las Leyes de Protección de Datos Personales informatizados, que nacen para proteger al titular de la información en lo que se refiere a su intimidad personal, *restringen la circulación no autorizada de datos* que puedan representar una invasión de la esfera privada.

En cuanto al procesamiento de datos personales como forma de amenaza seria al derecho a la intimidad, se ha exigido que los Estados de la Unión Europea y de EEUU, respondan al desarrollo tecnológico estableciendo marcos jurídicos con condiciones que regulen la creación de archivos, sin prohibirse de forma total el uso de datos personales, de manera que pueda garantizarse el derecho a la información, derivado del principio de libertad de expresión.

---

<sup>74</sup> RIASCOS GÓMEZ, LIBARDO ORLANDO, "La visión legal del habeas data en Latinoamérica y Europa", publicado en [www.informática-jurídica.com](http://www.informática-jurídica.com), accedido a través del sitio web: [http://www.informatica-juridica.com/trabajos/La\\_vision\\_legal\\_del\\_habeas\\_data\\_en\\_latinoamerica\\_y\\_europa.asp](http://www.informatica-juridica.com/trabajos/La_vision_legal_del_habeas_data_en_latinoamerica_y_europa.asp)

El enfoque estadounidense de los problemas generados por el tratamiento de datos de carácter personal difiere del de Europa continental y del adoptado en el orden internacional (global y regional europeo). Mientras en los Estados Unidos de América preponderantemente se ha recurrido sólo a regular esta temática cuando se lo consideró imprescindible y de manera limitada a través de leyes sectoriales (por ejemplo: The Privacy Act: ley sobre privacidad; the Freedom of Information Act: ley sobre libertad de información; the Fair Credit Reporting Act: ley sobre reportes de crédito, etcétera); en los países europeos se ha realizado una pormenorizada regulación por medio de leyes generales que prevén determinados órganos específicos de tutela<sup>75</sup>.

De hecho, el Parlamento Europeo ha trabajado arduamente en la cuestión, y a través del dictado de sucesivas directivas, ha logrado regular la protección de la intimidad en el entorno de las comunicaciones electrónicas de un modo exhaustivo, logrando ubicarse entre los países de legislación más avanzada.

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo de la Unión Europea dictaban la **Directiva 95/46/CE** relativa a

---

<sup>75</sup> PUCCINELLI, OSCAR RAÚL, "op cit" página 129.

*“protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos”*, sienta principios en torno al tratamiento informatizado o manual de datos personales, que tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos. Estas obligaciones, se refieren en particular, a la calidad de datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento. De otra parte, estos principios hacen referencia a los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, tales como, el de ser informados acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias.

Dicho cuerpo normativo fue una de las fuentes en las que se inspiró el legislador argentino para sancionar la Ley 25.326 sobre “Protección de Datos Personales y Habeas Data”.

El 15 de diciembre de 1997 dictaron la **Directiva 97/66/CE** sobre *“Protección de datos personales e Intimidad en las Telecomunicaciones”* que constituye una norma jurídica

comunitaria que traduce los principios de la **Directiva 95/46/CE** en normas concretas para el sector de las Telecomunicaciones. Además, tuvo como principal objeto el de reforzar las obligaciones de los Estados miembros en materia de confidencialidad. Esta directiva fue derogada y sustituida por la directiva que mencionaremos a continuación.

El 12 de julio de 2002 el Parlamento Europeo y el Consejo de la UE dictaron la **Directiva 02/58/CE** relativa al "*Tratamiento de los datos personales y a la protección de la Intimidad en el sector de las comunicaciones electrónicas*" para el respeto de la confidencialidad en la navegación en Internet. Esta directiva insta a los Estados miembros a armonizar las legislaciones nacionales respectivas para garantizar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales y, en especial, en lo que se refiere a su derecho a la intimidad informática, de forma que los datos personales puedan circular libremente por la comunidad. Esencialmente, impone a los proveedores de red y de servicios que los "*datos de tráfico*" (esto es "*cualquier dato tratado a los efectos de una comunicación a través de una red de comunicaciones electrónicas*") sean borrados o hechos anónimos cuando ya no se necesiten para la transmisión, salvo los datos necesarios para la facturación o los pagos por interconexión. Se

exige el “previo consentimiento” del titular para que los datos puedan tratarse con fines comerciales.

Por otro lado, los hechos históricos no son ajenos a la problemática del derecho sino que constituyen en muchas ocasiones la causa desencadenante de los cambios normativos. Tal es lo que ocurrió en Estados Unidos: la crueldad del atentado contra las torres gemelas de Nueva York del 11 de septiembre de 2001 provocó un cambio en la política de protección a la privacidad en las telecomunicaciones, motivado por el rediseño de la estrategia para combatir el terrorismo internacional. La **USA Patriot Act** dictada al mes de los atentados y prorrogada en marzo de 2006, otorga *amplias facultades de intromisión* en las comunicaciones electrónicas a las autoridades administrativas, afectando la privacidad de los datos personales. A la vez, fomenta la promoción del intercambio de datos entre las autoridades públicas y entre éstas con el sector privado; la generación de perfiles informáticos de los navegantes y *obliga* a los proveedores de comunicaciones y servicios en línea a *guardar datos de contenido y tráfico de sus usuarios*<sup>76</sup>.

---

<sup>76</sup> UICICH, RODOLFO DANIEL, “op cit” página 117.



El 13 de abril de 2006, tal vez bajo la influencia de lo ocurrido en EE.UU, el Parlamento Europeo y el Consejo de la UE dictan la **Directiva 06/24/CE** *“sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones”*. Esta directiva obliga a las compañías de telecomunicaciones a retener, por un período de entre seis y veinticuatro meses, numerosos datos de comunicaciones telefónicas y electrónicas dentro de la lucha contra el terrorismo. Sin embargo, se dijo que la protección de datos personales consagrada en las directivas 95/46/CE y 02/58/CE son plenamente aplicables a los datos conservados y si una persona sufre un perjuicio como consecuencia de un tratamiento ilícito tendrá derecho a obtener la reparación que le corresponda.

Por último, queremos mencionar un artículo de la Directiva 95/46/CE que mantuvo su vigencia a través de las sucesivas directivas y que tiene como base el principio de que “el ejercicio de los derechos no es absoluto”, dado que admite que los Estados miembros adopten *“medidas legales”* para limitar el alcance de los derechos y obligaciones previstos en la directiva a fin de *“proteger la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación*

*descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia”.*

Además, los datos sólo podrán conservarse durante un plazo limitado, justificado en los motivos antes mencionados.

En base a las citadas directivas los países europeos han ido adaptando sus legislaciones nacionales, existiendo al respecto un interesante repertorio de normas. Por razones de brevedad no nos detendremos a analizarlas, sólo nos ocuparemos en detalle de la regulación de la temática en el derecho argentino.

Sin duda alguna, los dilemas que plantea Internet constituyen un fenómeno actual y de aparente permanencia en el tiempo, que nos coloca ante el desafío de examinar la legislación vigente en nuestro país en materia de protección de datos, así como los instrumentos legales con que contamos los ciudadanos para velar por el respeto de nuestros derechos, y su operatividad o no de cara a los nuevos riesgos que supone la introducción de innovadoras tecnologías digitales. Allá vamos!!

### Regulación Normativa en el Derecho Argentino

En Latinoamérica la constitucionalización del Hábeas Data comenzó a finales de la década de los ochenta, en algunos pocos casos (v.gr. Brasil) y principios (v.gr. Colombia, Perú, Argentina y Ecuador) y finales de los noventa (v.gr. Bolivia y Venezuela) así como también principios del dos mil (v.gr. Panamá y Honduras).

En Argentina, el Habeas Data fue incorporado con la reforma constitucional de 1.994 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<sup>77</sup>.

El debate en el seno de la convención constituyente se centró en la preocupación por la libertad y seguridad personales. “La historia de la represión ilegítima en Argentina, recrudescida en la década de 1970, gravitaba con el peso de la violación de las garantías personales en el ánimo de los convencionales constituyentes, quienes procuraron poner remedio, en el futuro, a eventuales quebrantamientos de los derechos humanos. La obtención de certeza acerca de lo que el Estado conocía y asentaba sobre las personas, constituyó una prioridad para la seguridad de todos.

La instrumentación del habeas data como remedio a tales situaciones de desaparición forzada de personas, perfilaba un instituto jurídico sin duda singular, un instrumento llamado a condicionar el secreto de Estado sin por ello desproteger las necesidades sociales ni tampoco a la sociedad.

Sin embargo, el debate (y la norma que en definitiva resultó) fue virando desde la protección de la libertad personal hasta el control de la

---

<sup>77</sup> BIDART CAMPOS, GERMÁN J., “Tratado Elemental de Derecho Constitucional Argentino” Tomo II-A, Nueva Edición ampliada y actualizada a 2002-2003, Sociedad Anónima Editora, Comercial, Industrial y Financiera; página 310.

actividad desarrollada por otros operadores de datos, cuyos registros respondían a finalidades publicitarias, comerciales o financieras y a las eventuales interferencias en la vida privada de las personas, que esa actividad podía generar.

Así, de la protección y seguridad de las personas, afectadas por datos erróneos o falsos asentados en registros públicos, la nueva institución pudo contemplar el resguardo de derechos tales como la intimidad, la imagen, el buen nombre y fama comercial, la identidad personal y familiar a través de la regulación de un amparo especial, el hábeas data, denominado *nuevo derecho* en alguna de las intervenciones de los convencionales constituyentes<sup>78</sup>.

El habeas data significa, por analogía con el habeas corpus, que cada persona “tiene sus datos” (en vez de “tiene su cuerpo”). 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<sup>79</sup>.

---

<sup>78</sup> GELLI, MARÍA ANGÉLICA, “Constitución de la Nación Argentina. Comentada y Concordada”, Tomo I, Cuarta edición ampliada y actualizada, Editorial LA LEY, Buenos Aires, 2009, páginas 635 - 656.

<sup>79</sup> BIDART CAMPOS, GERMÁN J., “op cit” página 310. .

Se trata de un mecanismo de protección de la privacidad con el sentido tuitivo definido por la propia Corte Suprema de Justicia de la Nación en el caso "Ponzetti de Balbín", cuando sostuvo que la intimidad configura el "derecho a decidir por sí mismo en qué medio compartirá (la persona) con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal"<sup>80</sup>.

- Naturaleza Jurídica del Habeas Data:

Después de regular el amparo, el artículo 43 de la Constitución Nacional dispone que toda persona podrá interponer esa acción para tomar conocimiento de los datos a ella referidos.

Según María Angélica Gelli, "en la economía de la Constitución, el hábeas data es una especie de amparo. Amparo especial que no se confunde con el género desde que tiene especificidad propia, por lo que no constituye acción subsidiaria de otras. Además, por la peculiaridad de su finalidad, no requiere que quien haya registrado los datos y los transfiera o someta a alguna forma de tratamiento, haya obrado con arbitrariedad o ilegalidad manifiesta. Basta, por ejemplo, con que el dato

---

<sup>80</sup> Caso "Ponzetti de Balbín", (J.A. 1985-I-513).

sea erróneo y se transmita con negligencia para que la acción quede expedita”.

Asimismo, la citada jurista sostiene que “no se requiere el agotamiento de la vía administrativa previa, aunque resulta conveniente que el peticionante solicite al registro respectivo, la información necesaria, su finalidad y, en su caso, la rectificación, a fin de ser tomada en cuenta esa conducta previa, al momento de imponer las costas”<sup>81</sup>.

- Sujetos protegidos (legitimación procesal activa):

La norma constitucional ampara los derechos de las personas a conocer sus datos y eventualmente a solicitar medidas 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<sup>82</sup>.

---

<sup>81</sup> GELLI, MARÍA ANGÉLICA, “op cit” páginas 635 a 656.

<sup>82</sup> GELLI, MARÍA ANGÉLICA, “op cit” páginas 635 a 656. .

Del texto del art. 43 tercer párrafo CN surge que puede interponer la acción toda persona, con el objeto de:

- a. *Conocer* los datos a ella referidos y la finalidad de su almacenamiento;
- b. Exigir la *supresión, rectificación, confidencialidad o actualización* de esos datos.

▪ Los bancos de datos afectados (legitimación procesal pasiva):

Conforme lo establece la norma constitucional, los registros o bancos de datos pueden ser “*públicos*” o “*privados destinados a proveer informes*”.

Como bien afirma Bidart Campos, “acá estamos pensando ante todo en alguien que, como legitimado pasivo, puede ser demandado a través del hábeas data por la persona que titulariza los datos poseídos o colectados por ese mismo sujeto demandado”<sup>83</sup>.

Por “**registros o bancos de datos públicos**” debemos entender los existentes en los organismos del Estado, de cualquier naturaleza, ya que la ley no establece excepciones. Esto incluye no sólo

---

<sup>83</sup> BIDART CAMPOS, GERMÁN J., “op cit” página 323.



a las reparticiones de la Administración Pública Nacional centralizada, sino también a los entes descentralizados, autárquicos, empresas públicas y sociedades estatales, así como dependencias provinciales y municipales. Nos interesa destacar especialmente que la expresión “registros o bancos de datos públicos” no debe ser interpretada en el sentido de registros públicos, por oposición a registros reservados o secretos, ya que la norma se refiere a los titulares u operadores de los registros o bancos de datos<sup>84</sup>.

Esta ha sido la interpretación de la Corte Suprema de Justicia de la Nación en el caso “Ganora”, especialmente en los votos de los ministros Fayt, Boggiano, Petracchi y Bossert<sup>85</sup>.

En cuanto a los registros o **“bancos de datos privados destinados a proveer informes”**, el decreto reglamentario 1558/2001 los ha definido como aquellos que exceden el uso exclusivamente personal (terminología un tanto ambigua) y los que tienen como finalidad la cesión o transferencia de datos personales, sea a título

---

<sup>84</sup> MOLINA QUIROGA, EDUARDO, “Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material”; Ponencia presentada a la XIV Conferencia Nacional de Abogados “Por la plena vigencia de la Constitución Nacional” realizada en la ciudad de Paraná los días 1, 2 y 3 de mayo de 2003. Comisión n°1. Publicada en Infojus el 20 de mayo de 2003, accedido a través del sitio web: [http://www1.infojus.gov.ar/doctrina/dacc030027-molina\\_quiroga-proteccion\\_datos\\_personales\\_como.htm?2&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacc030027-molina_quiroga-proteccion_datos_personales_como.htm?2&bsrc=ci).

<sup>85</sup> “Ganora Mario F. y otra s/hábeas corpus”, Fallos 322:2139 (1990).

oneroso o gratuito. Parecen ser, básicamente, las empresas o personas individuales dedicadas a recolectar información personal para suministrarla a sus clientes. Es el caso de las empresas de informes comerciales o financieros que proveen a bancos, financieras, comercios y a quienes conceden crédito en general, información sobre situación patrimonial, reclamos pecuniarios judiciales o extrajudiciales, etcétera. También podrían incluirse otras entidades como los colegios profesionales, establecimientos educativos, clubes deportivos, etcétera.

Una interpretación literal del texto constitucional nos llevaría a sostener que los bancos de datos automatizados que generan las empresas en base a los rastros que dejamos al navegar por Internet, no estarían dentro del alcance de la garantía por cuanto el principal objetivo no es proveer informes al público. Tal interpretación colocaría a los usuarios en situación de desprotección total ante las grandes empresas transnacionales que obtienen cuantiosos beneficios económicos a partir de la recolección y transmisión de datos personales a terceros.

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.

Al respecto, afirma Bidart Campos: “cuando acaso un banco de datos que no tiene como finalidad el uso público provee información a terceros acerca de esos datos, no nos cabe duda que el habeas data queda habilitado”<sup>86</sup>.

En sentido análogo Gelli expresa lo siguiente: “Para resolver el problema, es relevante definir el destino del dato, cuyo conocimiento puede obtenerse por medio del hábeas data. En efecto, habilitaría la acción, cualquier expresión de información, cualquiera fuere el lenguaje o código con que se exteriorice, que se destine a redactar informes o a formar parte de informes para proveer a personas distintas del titular o usuario de datos”<sup>87</sup>.

---

<sup>86</sup> BIDART CAMPOS, GERMÁN J., “op cit” página 311.

<sup>87</sup> GELLI, MARÍA ANGÉLICA, “op cit” páginas 635 a 656.

- Derechos tutelados:

La norma constitucional tiende a proteger una multiplicidad de derechos, tales como: el derecho a la intimidad, a la identidad, a la imagen, al honor, a la verdad, a la igualdad, a la seguridad personal y patrimonial, etcétera. Como bien afirma Gelli, “la lista de derechos parece inacabable”.

Asimismo, en la actualidad hay autores que refieren al “*derecho a la protección de datos*” como un derecho autónomo. En relación a ello, consideramos interesante el modo en que lo define el Tribunal Constitucional Español, en el caso “**Defensor del Pueblo s/recurso de inconstitucionalidad**”, del 30 de noviembre de 2000: “*El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*”.

Se encuentra en juego el derecho personal en un doble aspecto: por un lado para impedir el tratamiento de datos personales sin consentimiento de aquél a quien pertenecen o a quien se refieren y, por

el otro, para controlar el uso que se hace de los datos y oponerse a que se utilicen con fines distintos de aquellos que justificaron su obtención<sup>88</sup>.

Por último, queremos destacar 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. Ejemplifica tal postura, la siguiente frase brindada por Bidart Campos: “*hay derechos nuevos, y contenidos nuevos en derechos viejos*”<sup>89</sup>.

### La Ley 25.326 de Protección de los Datos Personales

En Argentina, la Ley 25.326 de Protección de los Datos Personales sancionada el 4 de octubre de 2000 y promulgada parcialmente el 30 de octubre del mismo año, 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.

---

<sup>88</sup> Sentencia del Tribunal Constitucional de España del 30 de noviembre de 2000, en el caso “*Defensor del Pueblos/recurso de inconstitucionalidad*” publicado en Suplemento de Derecho Constitucional, La Ley, 15/VI/2001.

<sup>89</sup> BIDART CAMPOS, GERMÁN J., “op cit” página 314.

Al decir de Gelli: “La demora legislativa de más de seis años resultó beneficiosa en un punto, pues la interpretación doctrinaria y jurisprudencial fue abriendo para el hábeas data cauces de aceptación social ante las prevenciones que la garantía suscitó. El temor a que fuese cercenado el derecho a informar o a ser informado; a que cualquier tipo de archivo fuese examinado por orden judicial; a que se afectaran los bancos de datos periodísticos; o a que se entorpeciera el funcionamiento de los registros económicos o financieros, retrasaba la sanción de la ley. Entretanto, la jurisprudencia fue elaborando una doctrina que, si bien provisoria, al decir de la Corte Suprema en el caso “*Ganora*”, amplió los horizontes de la garantía. De tal modo, es posible examinar la norma sancionada, a la luz de los precedentes jurisprudenciales que interpretaron directamente el Art. 43 CN y evaluar la constitucionalidad y razonabilidad de la disposición legal”<sup>90</sup>.

La Ley 25.326 denominada “Ley de Protección de Datos Personales y Hábeas Data” 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

---

<sup>90</sup> GELLI, MARÍA ANGÉLICA, “op cit” páginas 635 a 656.

honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre” (Art. 1º).

En los párrafos que siguen realizaremos un análisis de la Ley 25.326 en relación con la temática que constituye el objeto del presente trabajo, destacando sólo los aspectos que consideramos de interés al efecto.

La ley comienza enunciando una serie de definiciones técnico-jurídicas aplicables al tratamiento de datos personales y al mejor entendimiento de su objeto y fines (define “datos personales”; “datos sensibles”; “archivo, registro, base o banco de datos”; “tratamiento de datos”; “responsable de archivo, registro, base o banco de datos”; “datos informatizados”; “titular de los datos”; “usuario de datos”; “disociación de datos”, las cuales fueron expuestas en el capítulo III del presente trabajo). Gelli critica la técnica legislativa, tildándola como “*deficiente*” por cuanto: “ordena determinados problemas en varias disposiciones, superponiendo criterios, reiterando conceptos, y al mismo tiempo, restringiéndolos, lo que produce un resultado confuso”<sup>91</sup>.

A continuación, la ley se ocupa de exponer los principios generales relativos a la protección de datos, éstos son:

---

<sup>91</sup> GELLI, MARÍA ANGÉLICA, “op cit” páginas 635 a 656.

- ✓ Licitud de las Bases de Datos: Serán lícitas cuando se encuentren debidamente inscriptas y se cumplan con los principios que establece la ley.
- ✓ Calidad de los datos: Los datos personales que se recojan deben ser **ciertos, adecuados, pertinentes y no excesivos** en relación al ámbito y finalidad para los que se hubieren obtenido; no pueden ser utilizados para finalidades distintas o incompatibles (Art. 4º inc.1 y 3). Aquí la ley introduce expresiones indeterminadas que dejan un peligroso margen de discrecionalidad. Además, creemos que la vaguedad del término “no excesivo” hace que en la práctica resulte difícil alegar y probar que la recolección de datos efectuada por el responsable del banco de datos supera la necesaria y por tanto, que es contraria a la ley. En cuanto a la utilización de datos para finalidades distintas, es frecuente la transgresión de la ley en éste punto, dado que los responsables de bases de datos manipulan los datos que recolectan con una multiplicidad de propósitos, y rara vez lo informan a sus titulares.  
  
Seguidamente se dispone: “Los datos **deben ser destruidos** cuando hayan dejado de ser necesarios o pertinentes a los fines



para los cuales hubiesen sido recolectados” (Art. 4º inc. 7). El decreto reglamentario 1558/2001 dispone que cuando el dato hubiera perdido vigencia respecto de los fines para los que fue obtenido debe ser **suprimido** por el responsable **sin necesidad de lo requiera el titular de los datos**. Este aspecto es también uno de los más vulnerados por parte de los responsables de bancos de datos automatizados, formados a partir de la recolección de los datos de navegación en Internet, por cuanto no se informa que están siendo recabados, no se solicita el consentimiento del usuario y en consecuencia tampoco se lo pone en conocimiento de los fines de la obtención, con lo cual difícilmente podamos saber cuándo son destruidos, o si son destruidos alguna vez.

- ✓ Consentimiento: La ley exige tanto para la obtención como para la cesión de datos personales “un **consentimiento libre, expreso e informado**, el que deberá constar **por escrito**, o por otro medio que permita se le equipare, de acuerdo a las circunstancias” (Art. 5 inc. 1). 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. Entendemos que el consentimiento del titular de los datos constituye, ni más ni menos, que un **aspecto capital** para determinar la licitud o ilicitud del banco de datos y la entidad de la obligación resarcitoria que puede recaer sobre su responsable por los daños ocasionados. Sobre este tema nos detendremos en el apartado que sigue.

- ✓ Información: Cuando se recaben datos personales se deberá **informar previamente** a sus titulares en **forma expresa y clara**: la finalidad para la que serán tratados, sus destinatarios, la identidad y domicilio de su responsable, el carácter obligatorio o facultativo de las respuestas, las consecuencias de proporcionar los datos o de la negativa a hacerlo, etcétera (Art. 6º). Consideramos acertada la inclusión de éste artículo por cuanto uno de los recaudos de licitud del consentimiento es que sea “**informado**”. Una vez más, se trata de un recaudo que es evadido habitualmente por los responsables de las bases de datos.
- ✓ Categoría de datos: La ley otorga una protección especial a los llamados “datos sensibles”, prohibiendo la obligación de proporcionarlos, así como la formación de archivos o bancos que

almacenen información que directa o indirectamente revelen tales datos (Art. 7º). Sin embargo, establece excepciones que hacen relativa tal prohibición.

- ✓ Datos relativos a la salud: Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes, respetando los principios del secreto profesional.
- ✓ Seguridad de los datos: Prohíbe registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad” (Art. 9).
- ✓ Deber de confidencialidad: El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al **secreto profesional** respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos...” (Art 10).
- ✓ Cesión: Exige el **previo consentimiento del titular de los datos**, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. El consentimiento para la cesión es **revocable**. Luego, se

mencionan excepciones a tal requisito y se establece también la responsabilidad solidaria entre cedente y cesionario en el cumplimiento de las obligaciones legales y reglamentarias (Art. 11).

- ✓ Transferencia Internacional: “Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados...” (Art. 12).

La ley consagra una serie de derechos en favor de los titulares de los datos, a saber:

- Derecho de Información: es aquél que tiene toda persona para solicitar información al organismo de control relativa a la existencia de bancos de datos personales, sus finalidades y la identidad de sus responsables. La información debe ser suministrada en forma clara, exenta de codificaciones y si fuera necesario acompañada de una explicación, en lenguaje accesible a todos. Asimismo, la información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular. No pueden revelarse datos pertenecientes a terceros en ningún caso (Arts. 13 y 15).

- Derecho de Acceso: El titular de los datos tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido o ante un informe que se considere “insuficiente” quedará expedita la acción de hábeas data (Art. 14).
- Derecho de rectificación, actualización o supresión: Es el derecho que tiene toda persona a que sus datos personales incluidos en un banco de datos sean rectificadas, actualizados, suprimidos o sometidos a confidencialidad, para lo cual el responsable cuenta con un plazo máximo de cinco días hábiles de recibido el reclamo del titular o advertido el error o falsedad. Si se incumple éste término, habilita al titular de los datos para que ejerza la acción de protección de los datos o Hábeas Data. (Art. 16 inc. 1 y 2). Al respecto, Gelli afirma: “Estimo que estas etapas (los diez días del art. 14 y los cinco días del art. 16) demoran innecesariamente la protección de los derechos, pues

si el titular del banco no rinde la información requerida, la acción de hábeas data podría incluir tanto el pedido de informes como las rectificaciones, actualizaciones, supresiones o confidencialidad que de probanzas resulte necesario adoptar<sup>92</sup>.

- Derecho a la impugnación de valoraciones personales: consiste en la facultad que tiene toda persona para impugnar una decisión judicial o un acto administrativo, cuando estas impliquen apreciación o valoración de la conducta humana que tengan como único fundamento el resultado de un tratamiento informatizado de datos personales. Será nulas las decisiones o actos que contravengan este derecho (Art. 20 incs. 1 y 2).

Al mismo tiempo, la ley estableció una serie de obligaciones precisas para los responsables de bases de datos personales: 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.

En cuanto a la recolección de los datos, están obligados a pedirle el consentimiento al titular e informarle sobre lo que pretenden

---

<sup>92</sup> GELLI, MARÍA ANGÉLICA, "op cit" páginas 635 a 656.

hacer con ellos para que, en última instancia, éste pueda decidir sobre la conveniencia o no de proporcionárselos. Tales datos deberán ser recolectados en forma lícita y leal y no ser utilizados para finalidades distintas de aquéllas para las que se recogieron, permitiéndole al titular poder acceder a los mismos cuando éste lo requiera para rectificar, cancelar o suprimir los datos que sean erróneos o falsos.

Finalmente, y con el fin de evitar la adulteración, pérdida o consulta no autorizada de los datos, los usuarios de los mismos tienen la obligación de adoptar medidas técnicas y organizativas que garanticen fehacientemente su seguridad y confidencialidad.

La correcta aplicación de todo este régimen se encuentra bajo la tutela de la mencionada Dirección Nacional de Protección de Datos Personales quien está facultada para sancionar el incumplimiento a la ley con apercibimientos, multas y la posibilidad de suspender o clausurar las bases de datos.

Pero además de estas sanciones administrativas, la norma creó nuevos delitos penales con prisión e inhabilitación especial para quienes accedan a un banco de datos de forma ilegítima o tras haber violado sistemas de confidencialidad y seguridad; para quienes inserten ilícitamente datos personales en un archivo; o quienes revelen

información de un banco de datos personal cuando por ley deban preservar el secreto.

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.

Nos basta con trazar el paralelo respecto del marco jurídico vigente en la Unión Europea para poner de manifiesto el grado de atraso que tiene nuestro país en lo que atañe a la regulación legislativa de ésta temática. De hecho, una de las fuentes de la mentada ley ha sido la Directiva 95/46/CE del año 1995, la que ha sido actualizada mediante la sanción de directivas posteriores. También se ha sostenido que nuestra ley *“no es más que una triste copia mal efectuada de la vieja LORTAD* (Ley Orgánica de Regulación del Tratamiento



Automatizado de los Datos de carácter personal) *española*<sup>93</sup>. Por lo tanto, acusa los mismos defectos de la LORTAD de 1992, y lo más grave es que desconoció las actualizaciones que la LOPDP (Ley Orgánica de Protección de Datos Personales) de 1999 de España<sup>94</sup>.

A su vez, al leer legislación comparada en la materia observamos como nota distintiva el hecho de que las mismas aluden a la “Protección de Datos Personales y **Privacidad**”. En efecto, las leyes europeas y en particular las alemanas se ocupan en detalle del resguardo de la privacidad de los usuarios de servicios de Internet. Allí radica, a nuestro entender, una de las principales falencias de la Ley 25.326 que ha quedado sin duda “obsoleta” como consecuencia del vertiginoso avance de la tecnología, la expansión mundial de Internet y el advenimiento de modernos métodos de captación, almacenamiento y transmisión de Datos Personales. Tales avances han facilitado la formación de bases de datos automatizadas a partir de la recolección y procesamiento de los datos de navegación de los internautas. Se trata

---

<sup>93</sup> MOEYKENS, FEDERICO RAFAEL, *Derecho a la libertad informática: consecuencias del Habeas Data*. Revista de Derecho Informático. Alfa-Redi n°046, Mayo de 2002.

<sup>94</sup> RIASCOS GÓMEZ, LIBARDO ORLANDO, “*La visión legal del habeas data en Latinoamérica y Europa*”, publicado en [www.informatica-juridica.com](http://www.informatica-juridica.com), accedido a través del sitio web: [http://www.informatica-juridica.com/trabajos/La\\_vision\\_legal\\_del\\_habeas\\_data\\_en\\_latinoamerica\\_y\\_europa.asp](http://www.informatica-juridica.com/trabajos/La_vision_legal_del_habeas_data_en_latinoamerica_y_europa.asp)

de nuevas situaciones que arroja el mundo virtual y que están lejos de hallarse contempladas por la ley argentina, tal como veremos en el apartado que sigue.

En este orden de ideas, Miguel Sumer Elias afirma: “Es indudable que la informática evoluciona y revoluciona de manera arrolladora llevándose por delante décadas de tradiciones y costumbres, y poniendo al derecho en jaque al desactualizar longevas normas jurídicas”<sup>95</sup>.

#### Aplicación de la Ley 25.326 a la nueva realidad que suscita Internet

En lo relativo a los aspectos informáticos es habitual que el ámbito de aplicación de la protección de datos sea delimitado en forma amplia, con lo que la Red entra de inmediato en escena. Así, la

---

<sup>95</sup> SUMER ELIAS, MIGUEL, “La Protección de Datos Personales en Argentina”, publicado en [www.informaticalegal.com](http://www.informaticalegal.com), accedido a través de: <http://www.informaticalegal.com.ar/2010/03/16/la-proteccion-de-datos-personales-en-argentina/>

normativa de protección de datos hay que considerarla aplicable a los datos personales que circulan por Internet<sup>96</sup>.

Hasta hace un tiempo, el foco de preocupación en torno a la invasión en el ámbito privado de los individuos lo constituía la violación de correspondencia privada, las interceptaciones telefónicas al margen de la ley; el seguimiento de comunicaciones a distancia; la fotografía clandestina tomada por la prensa. A todo ello, hoy en día debemos adicionarle: el acceso no autorizado a sistemas informáticos; la interceptación ilegal de correo electrónico; la suplantación de identidad digital; y en particular el rastreo de los datos de navegación que dejan los internautas y la formación de bancos de datos de carácter personal automatizados, que al aplicarle operaciones de tratamiento arrojan como resultado hasta los más ínfimos detalles de la vida de una persona. Esto último, se consigue a partir de la utilización de modernas tecnologías, tal como las ya mencionadas *cookies*.

Desde la óptica de la Ley 25.326, el responsable de la Base de Datos automatizada no cumple con las siguientes obligaciones legales:

---

<sup>96</sup> FERNÁNDEZ RODRIGUEZ, JOSÉ JULIO, "op cit" página 133.

- × 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.
- × No se efectúa un consentimiento libre, expreso, informado y por escrito que exige la ley.
- × No se informa al titular el hecho de que sus datos están siendo recolectados y mucho menos se le da a conocer las finalidades que se persiguen con ello. En consecuencia, se lo priva lisa y llanamente de los derechos de información, acceso, rectificación, actualización o supresión que la ley le garantiza.
- × Al carecer del consentimiento informado del titular de los datos, su recolección se concreta por medios desleales y fraudulentos.
- × Los datos recolectados no son destruidos, dado que los fines son abiertos y no se informan al titular, por ende 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.
- × No existe relación contractual, científica o profesional entre el titular de los datos y el responsable de la base de datos, de modo que no hay razón para excluir el consentimiento por parte

del titular. Distinto es el caso de los datos que proporcionan los usuarios a redes sociales como facebook en donde si existe relación contractual perfeccionada a través de un “contrato de adhesión”, de lo que nos ocuparemos más adelante.

- ✘ No se cumple con el deber de informar previamente al titular en forma expresa y clara de las circunstancias que enumera el art. 6º de la Ley 25.326.
- ✘ Debido a que a partir de los datos de navegación que recaban las cookies se puede llegar a conocer datos sensibles de personas identificables se está violando la prohibición que consagra el art. 7º de la Ley 25.326.
- ✘ 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.
- ✘ Se viola el deber de confidencialidad, cada vez que los datos personales son cedidos a terceros sin aplicar un procedimiento de disociación de la información que impida identificar a sus titulares.
- ✘ 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.

- ✘ Para el supuesto de que los datos sean recopilados para establecer perfiles determinados con fines promocionales, comerciales o publicitarios o para establecer hábitos de consumo, la ley exige que figuren en documentos accesibles al público o hayan sido facilitados por sus propios titulares u obtenidos con su consentimiento. Ninguna de las tres situaciones se dan en este caso, con lo cual se evidencia que la recolección de datos efectuada mediante la utilización de tecnologías como las cookies deviene **ILÍCITA**.
- ✘ Una vez más, por tratarse de bases de datos no inscriptas en el Registro que prevé la ley, las funciones y atribuciones de control con que cuenta la Dirección Nacional de Protección de Datos Personales carecen de operatividad atento a que resulta difícil verificar la observancia de las normas legales respecto de un archivo de datos cuya existencia se desconoce. Por esa misma razón, se encuentran exentos de la aplicación de sanciones

administrativas de apercibimiento, suspensión, multa, clausura o cancelación que prevé la ley. Tampoco encuadran en ninguna de las conductas tipificadas por los arts. 117 bis y 157 bis del Código Penal.

- ✘ Por último, queremos destacar que 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 (por no decir “imposible”) 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 la utilización de las llamadas *cookies*, 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.

## La importancia del Consentimiento en las operaciones de tratamiento de datos

Tal como se desprende del análisis de la Ley 25.326 las personas, en tanto somos titulares de los datos que nos conciernen, gozamos del derecho a controlar qué datos proporcionamos, a quiénes y con qué fines serán utilizados.

Se habla así actualmente del derecho a la “**autodeterminación informativa**” como la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos<sup>97</sup>.

Como bien afirma Guillermo Peyrano, “el principio del “consentimiento” es el pilar del sistema de protección de datos personales, toda vez que constituye la condición justificante de las

---

<sup>97</sup> VIGGIOLA, LIDIA E. y MOLINA QUIROGA, EDUARDO, “Tutela de la autodeterminación informativa. Aproximación a una regulación eficaz del tratamiento de datos personales”. Ponencia presentada al Congreso Internacional “Derechos y Garantías en el Siglo XXI” de la Asociación de Abogados de Buenos Aires.



operaciones de tratamiento a que pueden ser sometidos los datos, sin la cual las mismas quedan teñidas de ilicitud”<sup>98</sup>.

Su importancia radica en que constituye el medio o la modalidad a través de la cual el interesado tiene oportunidad de elegir el nivel de protección que le dará a la información sobre su persona, por eso debe tratarse de una expresión de voluntad consciente e informada<sup>99</sup>.

Al igual que todo acto voluntario, dicho consentimiento debe ser prestado con discernimiento, intención y libertad, de conformidad con lo dispuesto por el art. 897 del Código Civil.

Pero además, la Ley 25.326 en su artículo 5º exige como recaudo de licitud del tratamiento de datos personales que el titular hubiere prestado un consentimiento “**libre, expreso, informado y por escrito**” (u otro medio que permita se le equipare, de acuerdo a las circunstancias). Consideramos que se trata de una exigencia correcta y

---

<sup>98</sup> PEYRANO, GUILLERMO F, “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. Ingreso a Infojus el 22 de febrero de 2007, accedido a través de: [http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio\\_consentimiento\\_en\\_sistema.htm?3&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio_consentimiento_en_sistema.htm?3&bsrc=ci)

<sup>99</sup> GILS CARBO, ALEJANDRA M, “Régimen Legal de las Bases de Datos y Hábeas Data”, Editorial L. L., Buenos Aires 2001, pág. 78.

adecuada atento a que con el avance de la informática, la recolección y tratamiento de datos personales es moneda corriente.

Dada la importancia que la ley le otorga a tales recaudos a fin de determinar la licitud o ilicitud del tratamiento de datos, veamos qué aspectos comprende cada uno de ellos:

- ✓ Libre: Implica que el consentimiento debe responder a la auténtica voluntad de quien lo proporciona; libre de toda intimidación, fuerza, manipulación, coerción.
- ✓ Expreso: implica que debe ser prestado bajo las formas expresas de manifestación de la voluntad previstas en el art. 917 del Código Civil (verbalmente, por escrito o por signos inequívocos). El texto de la ley se ha inclinado por descartar el consentimiento manifestado en forma tácita o presunta.
- ✓ Por escrito: Se privilegia la declaración por escrito, respecto de los otros modos expresos de manifestación de la voluntad.

Seguidamente, la ley admite que se utilice *“otro medio que permita se le equipare, de acuerdo a las circunstancias”*.

“Sucedo que no puede soslayarse que los avances científicos, han impactado hondamente, tanto en las modalidades de manifestación de la voluntad, como en la comunicación de las

mismas, como así tampoco, que la registración, tratamiento y comunicación de datos personales, se realiza en la actualidad fundamentalmente, a través de medios informáticos.

En ese marco, deberán ser adoptados los recaudos técnicos que permitan garantizar la autoría de la declaración de voluntad a fin de tener por válidamente prestado el consentimiento, como asimismo que se haya cumplido con los requisitos de "libertad" e "información" a su respecto, requeridos por la ley<sup>100</sup>.

- ✓ Informado: se entiende por tal al que está precedido de una explicación al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que refiere el artículo 6º de la Ley N° 25.326 (así lo define el art. 5º del decreto 1558/2001). Es necesario destacar que cuando el art.6º de la ley 25.326 se ocupa de los alcances de este deber de "información", se refiere exclusivamente a la etapa de la "recolección" de los datos, y no incluye las demás operaciones comprendidas en el "tratamiento". Pese a ello, entendemos que la notificación al titular de los datos

---

<sup>100</sup> PEYRANO, GUILLERMO F, "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. Ingreso a Infojus el 22 de febrero de 2007, accedido a través de: [http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio\\_consentimiento\\_en\\_sistema.htm?3&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio_consentimiento_en_sistema.htm?3&bsrc=ci)

debe abarcar todas las etapas del procesamiento automatizado. Luego, la norma pone especial cuidado en aclarar, que cuando el consentimiento obre en otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información del art. 6º de la Ley 25.326. “El sentido de esta exigencia finca en descartar la posibilidad de la obtención de conformidades, conseguidas sin la cabal conciencia de los titulares respecto de su contenido y alcances”<sup>101</sup>.

En definitiva, el consentimiento libre, expreso e informado es requerido para el "tratamiento" de los datos de carácter personal, comprendiendo por ende todas las operaciones involucradas, tales como: la recolección, interrelación, intercambio y transmisión a terceros, cesión propiamente dicha, etcétera.

Por último, queremos destacar que la ley 25.326 incurrió en una seria omisión al no haber previsto la facultad del titular de revocar el consentimiento prestado, lo cual implicaba una injustificada limitación del poder de disponibilidad que sobre los datos se reconoce a sus

---

<sup>101</sup> PEYRANO, GUILLERMO F, “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. Ingreso a Infojus el 22 de febrero de 2007, accedido a través de: [http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio\\_consentimiento\\_en\\_sistema.htm?3&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio_consentimiento_en_sistema.htm?3&bsrc=ci)

titulares. La posibilidad de revocación del consentimiento, sólo se encuentra prevista en la ley 25.326 respecto del que fuera prestado en orden a la operación de "cesión" de datos (art.11 inc.2).

Sin embargo, en la reglamentación aprobada por el Decreto N° 1.558/2.001 se subsanó esta inadmisibles omisión, siguiéndose el criterio de la Ley Orgánica vigente en España, disponiéndose que "El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo", agregándose además que esa revocación "no tiene efectos retroactivos"<sup>102</sup>.

También es importante mencionar otra grave omisión en la que ha incurrido nuestra ley de protección de datos: nos referimos a la posibilidad para los titulares de ejercitar el denominado "**Derecho de Oposición**". Este derecho implica la posibilidad de oponerse al tratamiento de datos de carácter personal que se encuentren excluidos de la necesidad del consentimiento, invocando motivaciones fundadas y legítimas en base a las circunstancias concretas de cada caso.

---

<sup>102</sup> PEYRANO, GUILLERMO F, "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. Ingreso a Infojus el 22 de febrero de 2007, accedido a través de: [http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio\\_consentimiento\\_en\\_sistema.htm?3&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio_consentimiento_en_sistema.htm?3&bsrc=ci)

### El Contrato por Adhesión online

Al llevar adelante la presente investigación, hemos advertido que el consentimiento otorgado con las características antes mencionadas es poco habitual en nuestros días. Ocurre que al contratar servicios en la web, que pueden ir desde utilizar una página, un blog, una red social, efectuar compras online o simplemente navegar por Internet en búsqueda de la información que es de nuestro interés, frecuentemente se nos presentan términos y condiciones del sitio y políticas de privacidad que finalizan con un “ACEPTAR”, a lo que accedemos indefectiblemente por cuanto constituye la única opción que nos permite su utilización. 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, llamados comúnmente “Términos de Uso”, “Términos y Condiciones”, “Políticas de Privacidad”, es la de un **“Contrato por Adhesión”**.

Ossorio lo define así: “Constituye una típica y cada vez más frecuente modalidad de contratación, que se caracteriza por el hecho de que es una de las partes la que fija las cláusulas o condiciones, iguales

para todos, del contrato, cuya celebración se propone, sin que quienes quieran participar en él tengan otra alternativa que aceptarlo o rechazarlo en su totalidad, es decir, adherirse o no a los términos del contrato preestablecido, sin posibilidad de discutir su contenido”<sup>103</sup>.

El contrato de adhesión envuelve un consentimiento sin deliberaciones previas al aceptarse una formula preestablecida. Una de las problemáticas jurídicas que plantean estos contratos en Internet, es en cuanto a la verdadera configuración o no del “**consentimiento informado**” de los usuarios al aceptar las clausulas en el momento de la registración, ya que la mayoría de los usuarios no suelen leer los términos y condiciones del sitio web (generalmente son textos extensos, en letra chica e incluso suelen estar en idioma extranjero, resultando una lectura tediosa).

Se ha expresado que “no se trata de restarle validez al consentimiento del usuario expresado por medios electrónicos, el cual es perfectamente válido, sino de plantear la problemática típica de los contratos por adhesión llevada al ámbito de Internet en relación a la información necesaria que debe tener el usuario a fin de actuar con un

---

<sup>103</sup> OSSORIO, MANUEL, “Diccionario de Ciencias Jurídicas, Políticas y Sociales”, 33ª Edición Actualizada, corregida y aumentada por Guillermo Cabanellas de las Cuevas, Editorial Heliasta, Buenos Aires, 2008.

debido consentimiento informado en la manifestación de su voluntad al hacer click en “Acepto”<sup>104</sup>.

A su vez, otra cuestión central que se plantea es la “*jurisdicción pactada*” en los términos y condiciones, que generalmente es en países extranjeros. Ésta prórroga de competencia jurisdiccional impuesta por la parte dominante de la relación, hace que para el contratante débil (usuario) resulte inaccesible en virtud de la excesiva onerosidad.

Empero, en la jurisdicción argentina sería nulo, por tener objeto prohibido por el orden público, el contrato por el cual una empresa extranjera utiliza datos cuyo tratamiento está vedado por la ley del domicilio del titular de los datos (v. gr., los "datos sensibles" enumerados en el art. 2° de la ley 25.326); o sin haber obtenido el consentimiento del titular de los datos. Tal nulidad podría ser alegada por los usuarios en miras a proteger sus datos, pero una vez más el desconocimiento respecto de que sus datos están siendo sometidos a tratamiento les juega en contra.

De lo expuesto hasta aquí, podemos deducir fácilmente que de la suscripción de contratos de adhesión online se deriva la imposición de cláusulas a los usuarios que implican constantes violaciones a sus

---

<sup>104</sup> GONZALEZ FREA, LEANDRO, “op cit” página 5.



derechos personalísimos por parte de las grandes empresas que dominan la Red.

Tal es el caso de la Red Social Facebook, que cuenta actualmente con aproximadamente 900 millones de usuarios, y se ha convertido en una de las empresas que dispone de mayor volumen de información personal, proporcionada incluso por los propios usuarios. Por tal motivo, decidimos abocarnos a la lectura del contrato de adhesión que suscriben los usuarios al crearse una cuenta en la misma, con el convencimiento de que resultaría un buen ejemplo para finalizar la presente investigación.

Efectivamente, tal como lo imaginamos, el contenido de las cláusulas se encuentra diseñado en total detrimento de los derechos de los usuarios.

A continuación expondremos algunos aspectos que llamaron nuestra atención:

- × En los términos y condiciones se menciona que el acuerdo original *"se ha redactado en inglés de Estados Unidos"*, y continúa diciendo que *"en caso de existir discrepancias entre el original y una versión traducida, el original en inglés es el documento vinculante"*. Ya desde el inicio tal aclaración nos

resultó sumamente preocupante, por cuanto Facebook no garantiza que el acuerdo original (redactado en inglés) y la versión traducida (que es la que nosotros suscribimos) sean idénticos, resultando vinculante una versión del contrato que ni siquiera conocemos y que podría contener incluso, cláusulas totalmente dispares. Ante esta situación se nos plantean dudas sobre el papel que juega el consentimiento brindado por el usuario.

- × El acuerdo continúa con un apartado llamado "*Declaración de derechos y responsabilidades*", el cual contiene las condiciones de servicio que rigen la relación entre Facebook y los usuarios, como así también con todos aquellos que interactúan con dicha red social. Dentro de este apartado, se indica que "*al usar o al acceder a Facebook, muestras tu conformidad con esta Declaración, que se actualiza periódicamente*". Es decir, que el contrato se va actualizando, sin notificar al usuario y sin requerir un nuevo consentimiento. Asimismo, se deja sentado que el uso continuado de Facebook, después de los cambios en sus condiciones, constituye la aceptación de las enmiendas: esto implicaría un consentimiento tácito, que se aparta uno de los

recaudos de licitud del consentimiento respecto al tratamiento de datos personales: que sea “expreso”.

- × Se le otorga al usuario “*el poder de controlar el modo en que se comparte la información*”. Se pretende que sea el usuario el que se responsabilice en lo que respecta a la protección de su propia información. Nos cuesta creer que un ciudadano común, con conocimientos informáticos básicos, pueda tener realmente control sobre el destino que le depara a la información que publica. Además, “se supone” que es el responsable de la base de datos, en este caso Facebook, quien debe garantizar la seguridad, integridad y confidencialidad de los mismos (al menos así lo disponen la mayoría de las legislaciones nacionales).
- × El acuerdo señala que el usuario “*es el propietario de todo el contenido y la información que publica en Facebook*”, pero a continuación, establece que para el contenido protegido por derechos de propiedad intelectual, le concedemos a dicha red social lo que ésta llama “licencia de Propiedad Intelectual”: *le conferimos una licencia no exclusiva, transferible, con derechos de sublicencia, libre de derechos de autor para utilizar cualquier contenido de Propiedad Intelectual que publiquemos en*

*Facebook o en conexión con Facebook*". Se trata de una grosera violación a los derechos de propiedad intelectual de que gozan los autores de las publicaciones.

- × Posteriormente, el acuerdo establece que la licencia de Propiedad Intelectual *"finaliza cuando el usuario elimina el contenido o la cuenta, salvo si el contenido se ha compartido con terceros y éstos no lo han eliminado"*. Esto significa que Facebook no se responsabiliza en caso de que terceros no eliminen el contenido, por lo tanto, quien utiliza esta red social no es dueño de eliminar la información publicada cuando lo desea.
- × Para nuestra sorpresa, el contrato establece que Facebook **"no se compromete a garantizar la seguridad de los datos"**. Se desliga de tal responsabilidad imponiendo compromisos al usuario, tales como "no recopilarás información o contenido de otros usuarios"; "no molestarás, intimidarás ni acosarás a ningún usuario" o "no utilizarás Facebook para actos ilícitos, engañosos, malintencionados o discriminatorios". Facebook no sólo no controla el cumplimiento de los compromisos que impone, sino que tampoco cuenta con dispositivos que impidan, por ejemplo,

que un usuario descargue a su computadora fotos personales de terceros.

- × A lo largo de todo el acuerdo, Facebook indica "sus derechos" sobre las concesiones que hacen los usuarios, siendo los deberes o responsabilidades privativos sólo de estos últimos.
- × Se impone *jurisdicción extranjera* para cualquier demanda que se quiera entablar contra Facebook. A nuestro entender, esto implica un fuerte obstáculo para los usuarios de otras partes del mundo que quieran hacer valer sus derechos violados por acciones vinculadas a Facebook, jugando en su contra, para su defensa, el desconocimiento de la ley extranjera.
- × A continuación, establece que si alguien interpone una demanda contra Facebook relacionada con las acciones, contenido o información de uno como usuario, el mismo deberá encargarse de indemnizar a la red social y de librarla de la responsabilidad por todos los posibles daños, pérdidas y gastos de cualquier tipo relacionados con dicha demanda. Y sigue desligándose de responsabilidad, indicando que Facebook no controla ni dirige las conductas o acciones de los usuarios en la red social, no se responsabiliza por la información que los usuarios transmitan o

compartan, ni por los contenidos publicados que se consideren ofensivos, inapropiados, obscenos, ilegales o inaceptables. La idea central es siempre la misma: que la responsabilidad se traslade sólo a la otra parte.

- ✘ Llegando al final de la lectura del acuerdo, nos encontramos con una frase alarmante del mismo, la cual reza "*nos reservamos todos los derechos que no te hayamos concedido de forma expresa*".

De una u otra manera, vemos que Facebook siempre tiene **“derecho a todo”**, pero **nunca “se responsabiliza por nada”**.

Como se puede apreciar, 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.

La comercialización de datos personales en la Red es un **negocio en auge** que ha generado la aparición de empresas que se

dedican a procesar el comportamiento de los cibernautas.

La solución a esta problemática radica en la regulación de Internet de modo que permita equilibrar la posición asimétrica en la que se encuentran los usuarios en relación a las grandes corporaciones económicas. Se trata de una ardua tarea que requerirá indefectiblemente la cooperación entre el sector público y el sector privado y la intervención de los distintos actores implicados.

Todo esto sólo será operativo con la anuencia de los diversos Estados que, si bien se han visto superados con la supra territorialidad de Internet, siguen siendo los actores claves a la hora de la regulación jurídica en general.

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**<sup>105</sup>!!!

---

<sup>105</sup> CARR, NICHOLAS, "El gran debate sobre la privacidad en Internet", publicado en: [www.informaticalegal.com.ar](http://www.informaticalegal.com.ar), accedido a través de: <http://www.informaticalegal.com.ar/2010/09/04/el-gran-debate-sobre-la-privacidad-en-internet/>



## **CONCLUSIÓN**

A esta altura del desarrollo de nuestra investigación debemos confesar que iniciamos la misma con una visión un tanto ingenua en torno a la afectación del derecho a la intimidad perpetrada por las nuevas tecnologías. Al avanzar en el estudio de la temática planteada fuimos descubriendo distintas aristas que ponían en evidencia que tal afectación superaba todo lo imaginado.

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.

Por ello, sólo queremos destacar que 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, dando lugar a que los usuarios utilicen esta vía expedita para conocer y en su caso solicitar la supresión, rectificación, confidencialidad o actualización de sus datos personales que circulan en la Red, 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, nos resultó interesante y novedoso proponer como alternativa viable 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.

Los usuarios deberían tener el derecho, y no sólo la posibilidad, de retirar su consentimiento en relación al tratamiento de sus datos,

poniendo un freno a la propagación indefinida que caracteriza a la Red.

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

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Recomendaciones dirigidas a usuarios de Internet”, publicado en [www.agpd.es](http://www.agpd.es), accedido a través de: [https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/Recomendaciones\\_Internet\\_mayo\\_2006.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/Recomendaciones_Internet_mayo_2006.pdf)
  
- ARIAS, MARÍA CLARA, "¿Legal o ilegal? cómo funciona la venta de datos personales en Internet", 27 de julio de 2012, en la Página 24 Conurbano, consultado el 7 de marzo de 2013, accedido el 7 de marzo de 2013 a través de <http://24con.infonews.com/conurbano/nota/56632-legal-o-ilegal-como-funciona-la-venta-de-datos-personales-en-internet/>
  
- BIDART CAMPOS, GERMÁN J., “Repensando las garantías constitucionales”, “L.L”, 1991-B-977/8.
  
- BIDART CAMPOS, GERMÁN J., “Tratado Elemental de Derecho Constitucional Argentino” Tomo II-A, Nueva Edición ampliada y

actualizada a 2002-2003, Sociedad Anónima Editora, Comercial, Industrial y Financiera; página 310.

- BUERES, ALBERTO J. y HIGHTON, ELENA I., “Código Civil y normas complementarias. Análisis doctrinal y Jurisprudencial”, Tomo 3 A, editorial Hammurabi, 2005, página 137.
  
- CAO AVELLANEDA, Javier, "¿Puede Internet avasallar a la Justicia?", 12 de junio de 2010, en su blog personal "Apuntes de Seguridad de la Información" (Ingeniero en Informática, Consultor en seguridad de la información, CISA y Auditor ISO 27001), consultado el 8 de febrero de 2013, accedido el 8 de febrero de 2013, a través de la web <http://seguridad-de-la-informacion.blogspot.com.ar/2012/07/identidad-digital-y-reputacion-online.html>
  
- CAO AVELLANEDA, Javier, "Identidad digital y reputación online, la gestión de la e-privacidad", 27 de julio de 2012, en su blog personal "Apuntes de Seguridad de la Información" (Ingeniero en Informática, Consultor en seguridad de la información, CISA y Auditor ISO 27001), consultado el 8 de febrero de 2013,

accedido el 8 de febrero de 2013, a través de la web <http://seguridad-de-la-informacion.blogspot.com.ar/2012/07/identidad-digital-y-reputacion-online.html>.

- CAO AVELLANEDA, JAVIER, Identidad digital y reputación online, la gestión de la e-privacidad, publicado en el sitio web [www.informaticalegal.com.ar](http://www.informaticalegal.com.ar), accedido a través de: <http://www.informaticalegal.com.ar/2012/07/27/identidad-digital-y-reputacion-online-la-gestion-de-la-e-privacidad/>
- CARR, NICHOLAS, “El gran debate sobre la privacidad en Internet”, publicado en: [www.informaticalegal.com.ar](http://www.informaticalegal.com.ar), accedido a través de: <http://www.informaticalegal.com.ar/2010/09/04/el-gran-debate-sobre-la-privacidad-en-internet/>
- CIFUENTES, SANTOS, “Elementos de Derecho Civil Parte General”, editorial Astrea, Buenos Aires, 1997, páginas 150 y siguientes.

- Estudio sobre la privacidad de datos personales y la seguridad de la información en las redes sociales online. INTECO.
- 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, “Constitución de la Nación Argentina. Comentada y Concordada”, Tomo I, Cuarta edición ampliada y actualizada, Editorial LA LEY, Buenos Aires, 2009, páginas 635 - 656.
- GILS CARBO, ALEJANDRA M, “Régimen Legal de las Bases de Datos y Hábeas Data”, Editorial L. L., Buenos Aires 2001, pág. 78.
- GIULIANO, DIEGO ALBERTO, “El "habeas data" y la explotación de los datos personales: el caso argentino”, publicado en CUADERNOS CONSTITUCIONALES DE LA CATEDRA FADRIQUE FURIO CERIOL N° 32 . Departamento de Derecho

Constitucional y Ciencia Política y de la Administración de la Universidad de Valencia (España), 2000. Publicado en Infojus (Sistema de Información Jurídica) el día 13 de octubre de 2004.

- 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: <http://www.gonzalezfrea.com.ar/derecho-informatico/aspectos-legales-redes-sociales-legislacion-normativa-facebook-regulacion-legal-argentina/265/>
  
- HONDIUS F., "A decade of international Data Protection", Netherlands of International Law Review", vol 30, nº 2, 1983, página 105.
  
- LLAMBÍAS, J.J., Tratado de Derecho Civil Parte General I, editorial Perrot, 1967, página 275.



- MEYER, GRACIANA, "Entrevista al abogado Miguel Sumer Elías, especialista en Derecho Informático", 14 de diciembre de 2012, consultado el 7 de marzo de 2013, accedido el 7 de marzo de 2013, a través de la web "www.informaticalegal.com".
- MIRABELLI, "Banche dati e contemperamento degli interessi", *Banche dati telematica e diritti della persona*, Cedam, Padova, 1984, pág. 160.
- MOEYKENS, FEDERICO RAFAEL, Derecho a la libertad informática: consecuencias del Habeas Data. Revista de Derecho Informático. Alfa-Redi nº046, Mayo de 2002.
- MOLINA QUIROGA, EDUARDO, "Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material"; Ponencia presentada a la XIV Conferencia Nacional de Abogados "Por la plena vigencia de la Constitución Nacional" realizada en la ciudad de Paraná los días 1, 2 y 3 de mayo de 2003. Comisión nº1. Publicada en Infojus el 20 de mayo de 2003, accedido a través del sitio web:

[http://www1.infojus.gov.ar/doctrina/dacc030027-molina\\_quiroga-proteccion\\_datos\\_personales\\_como.htm?2&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacc030027-molina_quiroga-proteccion_datos_personales_como.htm?2&bsrc=ci).

- ORTI VALLEJO, A, “Derecho a la intimidad e informática”, Ed. Comares, Peligros (Granada), 1994.
- OSSORIO, MANUEL, “Diccionario de Ciencias Jurídicas, Políticas y Sociales”, 33º Edición Actualizada, corregida y aumentada por Guillermo Cabanellas de las Cuevas, Editorial Heliasta, Buenos Aires, 2008.
- PADILLA, MIGUEL M., “Bancos de Datos y Acción de Hábeas Data”, Editorial Abeledo Perrot, Buenos Aires, página 31.
- PALAZZI, PABLO ANDRÉS, en el artículo “El Hábeas Data en el Derecho Argentino”. Por Pablo Andrés Palazzi. Abogado. Coordinador del Posgrado en Derecho de la Alta Tecnología. Universidad Católica Argentina Facultad de Derecho. Profesor de Derecho Constitucional UCA (Argentina).

- PÉREZ LUÑO, ANTONIO E., “Los derechos humanos en la sociedad tecnológica”, en Mario Losano y otros, “Libertad informática y leyes de protección de datos personales”, CEC, Madrid, 1989, página 140.
- PEYRANO, GUILLERMO, “Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico”, publicado en EL DERECHO- Boletín N° 10.651, 13 de diciembre de 2002.
- PEYRANO, GUILLERMO F, “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. Ingreso a Infojus el 22 de febrero de 2007, accedido a través de: [http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio\\_consentimiento\\_en\\_sistema.htm?3&bsrc=ci](http://www1.infojus.gov.ar/doctrina/dacf070007-peyrano-principio_consentimiento_en_sistema.htm?3&bsrc=ci)
- PORRAS MARTINEZ, JOSÉ IGNACIO, “Los cambios tecnológicos y sociales que posibilitan la Organización en Red”, éste artículo fue presentado en forma en ponencia dentro del

Ciclo de Conferencias del Centro de Estudios del Comportamiento Organizacional (CECO), Universidad Bolivariana, el 3 de abril de 2001 y publicado en Revista de la Universidad Bolivariana Volumen 1 Número 2, 2001.

- Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid. Labor conjunta de los garantes de la privacidad de casi cincuenta países, bajo coordinación de la Agencia Española de Protección de Datos, accedido a través del sitio web:  
[http://www.agpd.es/portaleswebAGPD/canaldocumentacion/conferencias/common/pdfs/31\\_conferencia\\_internacional/estandares\\_resolucion\\_madrid\\_es.pdf](http://www.agpd.es/portaleswebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf)
  
- 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, pág. 122.

- RIASCOS GÓMEZ, LIBARDO ORLANDO, “La visión legal del habeas data en Latinoamérica y Europa”, publicado en [www.informática-jurídica.com](http://www.informática-jurídica.com), accedido a través del sitio web: [http://www.informatica-juridica.com/trabajos/La\\_vision\\_legal\\_del\\_habeas\\_data\\_en\\_latinoamerica\\_y\\_europa.asp](http://www.informatica-juridica.com/trabajos/La_vision_legal_del_habeas_data_en_latinoamerica_y_europa.asp)
  
- 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](http://vbn.aau.dk/files/62701961/SyD17_sal.pdf).
  
- SUMER ELIAS, MIGUEL, “La Protección de Datos Personales en Argentina”, publicado en [www.informaticalegal.com](http://www.informaticalegal.com), accedido a través de: <http://www.informaticalegal.com.ar/2010/03/16/la-proteccion-de-datos-personales-en-argentina/>

- TOMEIO, FERNANDO, Etiquetar una foto en Facebook puede afectar derechos personalísimos, publicado en La Nación, accedido a través de la web:  
<http://www.lanacion.com.ar/1441461-etiquetar-una-foto-en-facebook-puede-afectar-derechos-personalisimos>.
- TOMEIO, FERNANDO, Striptease digital y datos personales, publicado en La Nación, accedido a través de la web:  
<http://www.lanacion.com.ar/1503463-striptease-digital-y-datos-personales>
- TORNABENE, Inés, "Buscadores de Internet: ¿están o no obligados a filtrar contenidos injuriosos?", en HABEAS DATA Revista Electrónica del Centro de Protección de Datos Personales, 11 de diciembre de 2012, consultado el 7 de marzo de 2013, accedido el 7 de marzo de 2013, a través de la web <http://habeasdatacpdp.wordpress.com/tag/fallos-judiciales/>
- UICICH, Rodolfo Daniel, "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, consultado el

8 de febrero de 2013, accedido el 8 de febrero de 2013 a través de la web <http://www.madrid.org/>

- UICICH, RODOLFO DANIEL, El Derecho a la Intimidad en Internet y en las comunicaciones electrónicas, editorial Ad-Hoc, Buenos Aires, 2009.
- VIGGIOLA, LIDIA E. y MOLINA QUIROGA, EDUARDO, “Tutela de la autodeterminación informativa. Aproximación a una regulación eficaz del tratamiento de datos personales”. Ponencia presentada al Congreso Internacional "Derechos y Garantías en el Siglo XXI" de la Asociación de Abogados de Buenos Aires.

#### **JURISPRUDENCIA CITADA**

- Cámara en lo Civil y Comercial Federal, Sala Tercera de la Cámara en lo Civil y Comercial Federal, “Pamela David Gutiérrez c/ Microsoft de Argentina SA y su buscador de Internet, Bing”.
- 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>

- Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala I, "Prete Priscila c/ Yahoo de Argentina S.R.L. s/ daños y perjuicios", Causa N° 9847/2007, fallo del 06/09/2012, accedido en <http://www.paradigmadelderecho.com.ar/web/?p=5111>, publicado el 21/09/2012.
- Cámara Nacional de Apelaciones en lo Civil, Sala B, 14-11-2008, "Resnik, Cristian c/ Ideas del Sur S.A. s/ daños y perjuicios".
- 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/](http://www.hfernandezdelpech.com.ar/)
- Cámara Nacional de Apelaciones en lo Civil, Sala K, 9-12-99, "Labi, Sergio Juan c/ Editorial Perfil S.A. s/ daños y perjuicios", fallo del 09/12/1999, accedido en <http://ar.vlex.com/vid/labi-sergio-juan-editorial-perfil-perjuicios-35395561>



- Cámara Nacional de Apelaciones en lo Civil, Sala M, “Polino, Marcelo Alejandro c/ Editorial Televisa Argentina S.A. y otro s/ daños y perjuicios”, fallo del 07/10/2011, accedido en [www.paradigmadelderecho.com.ar/web/?p=2008](http://www.paradigmadelderecho.com.ar/web/?p=2008), publicado el 03/02/2012.
  
- “*Ganora Mario F. y otra s/hábeas corpus*”, Fallos 322:2139 (1990).
  
- "Ponzetti de Balbín, Indalia c. Editorial Atlántida, S.A. s/ daños y perjuicios", fallo del 11/12/1984, accedido en [notasfallosconstitucionaluba.blogspot.com.ar](http://notasfallosconstitucionaluba.blogspot.com.ar)
  
- Sentencia del Tribunal Constitucional de España del 30 de noviembre de 2000, en el caso “*Defensor del Pueblos/recurso de inconstitucionalidad*” publicado en Suplemento de Derecho Constitucional, La Ley, 15/VI/2001.



