UNIVERSIDAD ABIERTA INTERAMERICANA

Facultad de Derecho y Ciencias Políticas

Sede Regional Rosario

TESIS DE GRADO DE LA CARRERA DE ABOGACÍA

2007

Tutor: **Dr. Guillermo Beltramone**

Alumno: **Nicolás Matías Bistotto**

Tema: **"INTIMIDAD Y TECNOLOGIAS DE LA INFORMACION: Una mirada a los desafíos del nuevo milenio".**

Fecha de presentación: **18 de mayo de 2007.-**

Agradecimientos

A mis padres, por el apoyo incondicional que me brindaron siempre y en todo momento.

A Eliana, por su ayuda constante en cada etapa de mi carrera.

A Pili, mi compañera de estudio.

Y a todas aquellas personas que de algún modo colaboraron para hacer realidad este logro.

Finalmente agradecer al Dr. Guillermo Beltramone por su dedicación y esfuerzo que fueron de especial importancia para la elaboración de esta obra.

1.- Título:

Las bases de datos y su amenaza sobre el derecho a la intimidad

2.- Tema:

"INTIMIDAD Y TECNOLOGIAS DE LA INFORMACION: Una mirada a los desafios del nuevo milenio"

3.- Problema:

¿Cuáles son los efectos de la manipulación de bases de datos en Internet sobre el derecho a la intimidad?

4.- Objetivos

4.1.- Objetivos generales:

4.1.1.- Demostrar que el derecho a la intimidad es seriamente vulnerado y avasallado a través del tratamiento de bases de datos en Internet.

4.1.2.- Indagar las razones por las cuales en nuestro país no se logra aún un orden normativo acorde al avance de la informática.

4.1.3.- Describir los efectos positivos y negativos que arribaron con las nuevas tecnologías a nuestro sistema jurídico.

4.2.- Objetivos específicos:

4.2.1.- Analizar la vulnerabilidad a la que está expuesto el derecho a la intimidad.

4.2.2.- Contextualizar la situación actual de las bases de datos en nuestro país.

4.2.3.- Profundizar sobre lo concerniente a la informática y a las nuevas tecnologías en relación al Derecho.

4.2.4.- Brindar un panorama sobre la situación actual de la garantía constitucional de hábeas data en el sistema jurídico argentino.

5.- Hipótesis:

Es de imperiosa necesidad el dictado de leyes que vayan de la mano con los avances de las nuevas tecnologías, como así también el logro de una aplicabilidad total de la ley 25.326.-

Introducción

El derecho a la intimidad es el principal estandarte de los derechos personalísimos de una persona. La intimidad constituye la faz privada, y porque no, sagrada de todo ser humano. Lugar en el cual ninguna autoridad pública o privada debería tener acceso alguno. Derecho que por su condición de tal debe ser tutelado y protegido de toda vulneración o violación, más aún en tiempos como los que hoy se vislumbran, potenciados de un abismal y voraz avance tecnológico.

La tecnología llegó para quedarse, sobre todo en lo que a medios y nuevas formas de comunicación se trata. Este desembarque fue recibido con gran esperanza y entusiasmo por parte del ser humano, lo mismo que cada cambio, que sobre esta materia, día a día se va experimentando.

En medio de esa algarabía, sin que nadie lo advirtiese, la tecnología, de la mano principalmente de Internet, abrió puertas hacia la comunicación global pero también hacia la propia intimidad de las personas.

Despojó todo posible manto de hermetismo y privacidad que reposaba sobre cada individuo y comenzó, de alguna manera, a ser una cámara espía de cada uno de nuestros movimientos y prácticas, tanto públicas como también de aquellas que deberían quedar a resguardo en la faz interna de cada uno.

Algo que aparentaba ser “la gran herramienta de progreso”, fomentando la conectividad y la interacción global, derribando fronteras y acercando culturas, por momentos se torna perversa y provocativa. Si bien no podemos negar que Internet se ha vuelto una figura indispensable e imprescindible en estos días, sólo ha dejado sombras y leves rastros de aquella “ingenua” imagen que podía o de hecho llegó a manifestar en sus comienzos.

Estamos transitando a través de la tan conocida “era de la información”, en donde parece no existir límites, lo cual conlleva a la errónea idea o pensamiento que la persona, como ente social en sí, debe adaptarse sin queja alguna a los cambios que se suscitan en el mundo de la Internet sin la más mínima posibilidad de confrontar con ese avance que no da tregua.

Vivimos inmersos en un proceso constante y definido hacia el futuro que avasalla y no deja lugar alguno para la reflexión, cuestiones que son el basamento para la construcción de un orden normativo actual, eficiente y eficaz, que se adapte concomitantemente con los cambios que se van sucediendo.

En el presente trabajo quisimos expresar como se ha ido gestando este cambio, que por cierto no es abarcativo de una generación en particular, sino de la sociedad en su conjunto. Un cambio que fue, como es normal y predecible, transitando diversas etapas hasta llegar a lo que hoy en día se puede observar.

El Derecho no ha ido transformándose conjuntamente, lo cual plantea un interesante punto de discusión en torno a que grado de adaptación debería implementar o cual debería ser el ritmo de avance lógico, teniendo en cuenta que frente a éste se sitúa la tecnología, que crece y cambia constantemente.

A lo largo de los capítulos trataremos de demostrar las cuestiones que han sido planteadas, como así también indagar en torno a qué se está haciendo en materia legislativa para acompañar este cambio y fenómeno social, con el fin que el Derecho como tal no quede desactualizado y a la deriva frente a esta situación.

Puntualmente nos adentraremos en el derecho a la intimidad, para conocer mejor su contenido y su premisa de protección. Luego proseguiremos con lo que respecta a bases de datos, enfocándonos sobre su regulación y contenido, haciendo hincapié en la influencia o los efectos que Internet provoca sobre este tema. Abordaremos en profundidad la garantía constitucional del hábeas data, herramienta por excelencia y específica en lo que a bases de datos respecta. Y por último, analizaremos el cuerpo normativo que reglamenta dicha figura, como es la Ley de Protección de los Datos Personales (25.326).

Con este bagaje de información pretenderemos analizar el tema en cuestión, para que una clara comprensión del mismo funcione como disparador de posibles soluciones a los problemas que se plantean en la actualidad o que podrían llegar a suscitarse en un futuro próximo.

Capítulo I

DERECHO A LA INTIMIDAD

SUMARIO: 1. Introducción; 2. Concepto; 3. Evolución histórica; 4. Delimitación del ámbito privado y del público; 4.1. Acciones privadas internas; 4.2. Acciones privadas externas; 4.3. Acciones públicas; 5. Intimidad y hábeas data en la Argentina; 6. Antecedentes normativos; 7. La reforma constitucional de 1994; 8. El derecho a la intimidad en las fuentes internacionales constitucionalizadas; 8.1. Declaración Americana de los Derechos y Deberes del Hombre; 8.2. Declaración Universal de los Derechos Humanos; 8.3. Pacto Internacional de Derechos Civiles y Políticos; 8.4. Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica); 8.5. Convención sobre los Derechos del Niño; 9. Protección de datos personales.-

1.- Introducción

Vivimos en la llamada *"*sociedad de la información*"* o "era de la información", donde las potentes tecnologías de la informática y las comunicaciones permiten la acumulación y transmisión de datos a velocidades de micro segundos y en cantidades de imposible percepción para la mente humana. Aunque a primera vista este tema pueda parecer una cuestión sin implicancias jurídicas, veremos que la recopilación de dichos datos colisiona directamente con el derecho a la intimidad.

El gran avance de la tecnología informática en nuestras vidas ha hecho surgir un nuevo escenario jurídico.[1] El almacenamiento y el tratamiento de los datos de las personas son hoy parte destacada de este fenómeno técnico-social, que se desborda hacia el Derecho en busca de soluciones a sus conflictos.[2]IERINI

Ingresando en lo que tiene que ver con la regulación constitucional del derecho a la intimidad, hay que expresar que el art. 19, parte 1ª, de la Constitución Nacional establece la privacidad de las acciones de los hombres.[3]

Una primera lectura de la norma, que reconoce el denominado derecho a la privacidad o a la intimidad, parece llevar a concluir que el mundo privado de toda persona es una zona metajurídica, extraña al derecho, donde no llega el poder de la ley. La Corte Suprema de Justicia Nacional ha dicho que "*las acciones privadas quedan fuera de la competencia del ordenamiento jurídico; podrán estimarse buenas o malas, pero no admiten la calificación de lícitas o ilícitas según el derecho"*.[4]

Sin embargo, el mundo privado no es una esfera ajena al derecho. Según el principio de que "lo no prohibido está permitido" -que enuncia la última parte del art. 19 de la Constitución Nacional- resulta que la intimidad de una persona es una zona intrínsecamente lícita, que merece respeto y protección. El criterio de la mayoría de la Corte Suprema se inclina hacia la siguiente tesis: en concreto, "…*el Estado debe realizar la protección de la privacidad, comenzando por no entrometerse en ella, respetando el área de inmunidad de toda persona…"*.[5] SAGUES

2.- Concepto

El respeto a la intimidad de la vida privada constituye uno de los llamados derechos de la personalidad, conjuntamente con el derecho a la vida, a la integridad física, a la libertad, al honor y a la disposición del propio cuerpo.[6] El derecho a la intimidad se halla en la esfera secreta e interna de la propia persona y se le conoce en el derecho anglosajón como "right of privacy", y en Italia como "diritto alla riservatezza".[7]

Es el derecho a exigir el respeto de la vida privada y familiar de cada persona, garantizándose el normal desenvolvimiento y la tranquilidad particular, sin que en modo alguno, y fuera de los casos permitidos por la ley, se admitan intromisiones extrañas.[8]

También se ha entendido al derecho a la intimidad como el derecho personalísimo que permite sustraer a la persona de la publicidad o de otras turbaciones a la vida privada, el cual está limitado por las necesidades sociales y los intereses públicos.[9]

La intimidad no debe reducirse a no ser molestado, a no ser conocidos en algunos aspectos por los demás, sino que abarca el derecho a controlar el uso que otros hagan de la información concerniente a un sujeto determinado. Es la zona de reserva libre de intromisiones que rodea al individuo.[10] Es una necesidad del hombre en su intento por vivir en un marco de dignidad, igualdad y libertad que le permita un desarrollo integral de su personalidad.[11]

La Corte Suprema de Justicia Nacional expresó que *"en la era de las computadoras el derecho a la intimidad ya no puede reducirse a excluir a los terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal que de él figura en los registros, archivos y bancos de datos".*[12]

E

3.- Evolución Histórica

Debemos remontarnos a la Edad Antigua para encontrar las primeras manifestaciones de la intimidad y su trascendencia respecto a la vida individual y social de la persona.

En Grecia no se entendía una separación entre lo público y lo privado -o propio- de cada individuo, en consecuencia, esta concepción de ciudadanía del mundo griego influyó negativamente en la construcción del mundo familiar y personal, pues los aspectos más interiores de la vida humana quedaban a merced del Estado y sus leyes.

Si bien no era posible la configuración de un derecho a la intimidad tal como en la actualidad se entiende, ello no significaba que no existiera, sino que era eficazmente reprimido por la exigencia de participación en la vida de la polis.[13]

Esta concepción sobre el derecho a al intimidad desapareció en el mundo romano, en donde su reconocimiento estaba dado por la protección jurídica del domicilio y la correspondencia. No obstante, se evidenciaba en algunas normas legales el desprecio por la intimidad de la persona, por ejemplo en la ilegalidad de los matrimonios entre personas de edad avanzada.

Pero en definitiva, la idea de intimidad estaba presente entre los romanos y adquirió mayor significación que la que tuvo en el mundo griego. Ya en la Edad Media gravitaron en el desarrollo del concepto de intimidad la influencia romana, la expansión del mundo germánico y el pensamiento cristiano.[i]

En esta época el derecho a la intimidad se halló estrechamente ligado al nacimiento de la burguesía. Pero la intimidad, considerada como un conjunto de facultades o poderes atribuidos a su titular aparece recién cuando se disgrega la sociedad feudal, en la cual siguiendo a la polis o a la civita del mundo antiguo, los individuos se hallaban insertos en la sociedad o comunidad y vinculados entre sí por una intrincada red de relaciones que se reflejaban en todos los aspectos de su vida cotidiana.[15]

La intimidad llega entonces, junto con el surgimiento de la burguesía; cuando esta nueva clase social aspiraba a acceder a lo que antes había sido un privilegio de unos pocos. Esta realidad muestra un marcado matiz individualista, ya que la idea de intimidad estaba pensada para el disfrute de un grupo selecto, sin que existiera la inquietud de hacerla llegar a las clases humildes de la población.

A fines del siglo XIX, en Estados Unidos, se sentaron las bases jurídicas de la ″privacy″, concibiéndola como el derecho de la soledad y garantía del individuo a la protección de la persona y de su seguridad, frente a la invasión del sagrado recinto de su vida privada y doméstica.[16]

En el siglo XX, ″la privacy″, esa noción anglosajona análoga a nuestro concepto de derecho a la intimidad, ha asumido un papel ambivalente:

a) ha sido esgrimida con la intención conservadora de no proporcionar a los poderes públicos informaciones económicas con el propósito de evadir impuestos;

b) por otro lado, con el advenimiento de la informática, se ha utilizado desde posiciones progresistas para reaccionar contra la acumulación de datos destinados al control de comportamientos ideológicos o información sensible con fines discriminatorios.

En este contexto el derecho a la intimidad ha adquirido rango constitucional y ha perdido su exclusivo carácter individual y privado para asumir progresivamente un rol de significación pública, colectiva y social.[17]

El problema del suministro de datos personales dejó de ser una cuestión de interés únicamente para la alta burguesía y atañe hoy, por efecto de la proliferación de bancos de datos y la recolección informática de datos personales, a todas las personas, con independencia de su situación económica o social.[18]

4.- Delimitación del ámbito privado y del público

En el derecho argentino es posible detectar tres tipos de conductas en orden a diferenciar lo privado de lo público, y, en base a esto, determinar el grado de incidencia de un accionar sobre la esfera íntima de una persona.

4.1.- Acciones privadas internas

Son los comportamientos privados en sentido estricto (conductas íntimas o inmanentes), ya que principian y concluyen en el sujeto que las realiza. No trascienden de él. Comprenden aquellos hechos realizados en absoluta privacidad o de los que nadie puede percatarse (por ejemplo, el mero acto de pensar).

Estas acciones están expresamente tuteladas por el art. 19 de la Constitución Nacional, aunque también por el 18 -cuando trata la inviolabilidad del domicilio y papeles privados-. Merecen un completo respeto por parte del Estado y de los particulares.[19]

4.2.- Acciones privadas externas

Son comportamientos que trascienden al sujeto que las realiza y, por tanto, son conocidas por los demás; pero no interesan al orden y a la moral pública, ni causan perjuicio a terceros. Dicho de otro modo, no afectan al bien común. A los fines del art. 19 de la Constitución Nacional son también acciones privadas, con la misma tutela a favor de quien las lleva a cabo.[20]

4.3.- Acciones públicas

Son acciones externas, ya que trascienden a quien las ejecuta y, además, preocupan al bien común -en particular, porque pueden comprometer el orden o la moral pública, o causar daño a terceros-. Son regulables por el Estado y aún prohibidas por éste de haber motivos para ello.[21]

5.- Intimidad y hábeas data en la Argentina

Argentina recibió un fuerte legado cultural a través de las tradiciones jurídico-políticas heredadas de España en la época de la colonización y que se mantuvieron a través del tiempo. El sistema jurídico argentino recibió la influencia de la inquisición española que se manifestó en el monopolio estatal de la registración de datos de la vida y propiedades de los súbditos del Estado.

Durante mucho tiempo, la información era conservada en manos de una minoría aristocrática que tenía acceso a la cultura, mientras el resto de la población vivía en un total estado de desinformación.

Nuestra Constitución Nacional de 1853 no menciona la palabra intimidad ni privacidad, pero la doctrina y la jurisprudencia le han reconocido rango constitucional por medio del art. 19. A su vez, el art. 18 contiene disposiciones que contemplan aspectos importantes de este derecho, tales como la inviolabilidad de domicilio, correspondencia y papeles privados.[22]

Tomando como base las normas de nuestra Carta Magna, la Corte Suprema de Justicia[23] definió con amplitud el derecho a la intimidad consagrado en el art. 19, amparando la autonomía individual integrada por los sentimientos, hábitos, costumbres, relaciones familiares, posición económica, creencias religiosas, salud mental y física junto a todos los hechos y datos que integran el estilo de vida de una persona que la comunidad considera reservados al individuo y cuyo conocimiento y divulgación significa un peligro para su intimidad.

6.- Antecedentes normativos

En nuestro país, el IV Congreso Nacional de Derecho Civil que tuvo lugar en el año 1969 aprobó un despacho sobre el tema: “Los derechos de la propiedad y su protección legal”, recomendando que se incluyan en el Código Civil o en leyes especiales preceptos que regulen las consecuencias civiles del principio constitucional del respeto a la personalidad humana, como pueden ser, entre otros, los relativos a los derechos a la intimidad, a la imagen y a la disposición del

propio cuerpo. Recién en 1974 se dictó la ley 20.889[24] que incorporó al Código Civil el artículo 32 bis sobre el derecho a la intimidad.

Esta ley tuvo una irregular tramitación en el Congreso de la Nación y dicha circunstancia dio motivo al dictado de la ley 21.173, promulgada el 15 de octubre de 1975, que derogó la ley anterior -y por lógica el citado artículo- y dispuso que se incorporase al Código Civil el artículo 1071 bis[25], que en materia civil, brinda la protección a la intimidad de la persona.

Dicho artículo se asienta sobre cuatro pilares fundamentales:

*Quien efectúe una intromisión arbitraria en la vida ajena;
* Publicando retratos, difundiendo correspondencia, perturbando la intimidad;
* Deberá cesar en la acción, o
* Pagar una indemnización.

La intromisión en la vida ajena debe ser arbitraria, ya que en numerosos casos de ejercicio legítimo de un derecho o de cumplimiento de una obligación legal se causan mortificaciones y aún daños que no comprometen la responsabilidad del agente, en tanto obre dentro de los límites de su derecho u obligación.

Cualquier acto de intromisión en la vida privada ajena es motivo de la previsión legal, sea que consista en publicación de retratos, divulgación de correspondencia, u otra forma de mortificación en las costumbres o sentimientos, de tal modo que se perturbe la intimidad de otro.

El dispositivo legal funciona para hacer cesar la intromisión y ordenar las indemnizaciones correspondientes si del hecho hubieran resultado daños materiales y, obviamente, la reparación del daño moral que según las circunstancias parece que ineludiblemente se ha de producir. Para la más adecuada reparación puede el juez, a pedido de parte, ordenar la publicación de la sentencia en un diario o periódico del lugar.

7.- La reforma constitucional de 1994

La Constitución Argentina reformada en 1994 incluye al hábeas data en el tercer párrafo del artículo 43[26], dentro del marco de la acción de amparo y entendiéndoselo como una especie del mismo, sin darle expresamente ese nombre.

La existencia de este instrumento constitucional es un gran avance para la protección del derecho a la intimidad en lo relativo a la protección de datos personales. Ahora bien, el hecho de contar con un artículo de semejante magnitud en nuestra Carta Magna hacía necesaria una ley que desarrolle dicho precepto constitucional. Y dicha ley llegó, bajo el número 25.326, y más tarde, su correspondiente decreto reglamentario 1558/2001.

8.- El derecho a la intimidad en las fuentes internacionales constitucionalizadas

Los tratados de derechos humanos constitucionalizados por el artículo 75, inc. 22[27] de la Constitución Nacional, a partir de la reforma de 1994, regulan los aspectos relacionados con la privacidad de la siguiente manera:

8.1.- Declaración Americana de los Derechos y Deberes del Hombre

Art. V. – "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

Art. IX. – "Toda persona tiene el derecho a la inviolabilidad de su domicilio".

Art. X. – "Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia".[28]

8.2.- Declaración Universal de los Derechos Humanos

Art. 12. – "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 injerencias o ataques".[27]

8.3.- Pacto Internacional de Derechos Civiles y Políticos

Art. 14. - 1. "Todas las personas son iguales ante los tribunales y cortes de justicia. Toda persona tendrá derecho a ser oída públicamente y con las debidas garantías por un tribunal competente, independiente e imparcial, establecido por la ley, en la substanciación de cualquier acusación de carácter penal formulada contra ella o para la determinación de sus derechos u obligaciones de carácter civil. La prensa y el público podrán ser excluidos de la totalidad o parte de los juicios por consideraciones de moral, orden público o seguridad nacional en una sociedad democrática, o cuando lo exija el interés de la vida privada de las partes o, en la medida estrictamente necesaria en opinión del tribunal, cuando por circunstancias especiales del asunto la publicidad pudiera perjudicar a los intereses de la justicia; pero toda sentencia en materia penal o contenciosa será pública, excepto en los casos en que el interés de menores de edad exija lo contrario, o en las acusaciones referentes a pleitos matrimoniales o a la tutela de menores..."

Art. 17. – 1. "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".[29]

8.4.- Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica)

Art. 8. - ...

2. ...

d) "derecho del inculpado de defenderse personalmente o de ser asistido por un defensor de su elección y de comunicarse libre y privadamente con su defensor..."

Art. 11. - ...

2. "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 o reputación".

3. "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".[30]

8.5.- Convención sobre los Derechos del Niño

Art. 16. - 1. "Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación".

2. "El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

Art. 40. - 1. "Los Estados Partes reconocen el derecho de todo niño de quien se alegue que ha infringido las leyes penales o a quien se acuse o declare culpable de haber infringido esas leyes a ser tratado de manera acorde con el fomento de su sentido de la dignidad y el valor, que fortalezca el respeto del niño por los derechos humanos y las libertades fundamentales de terceros y en la que se tengan en cuenta la edad del niño y la importancia de promover la reintegración del niño y de que éste asuma una función constructiva en la sociedad".

2. "Con este fin, y habida cuenta de las disposiciones pertinentes de los instrumentos internacionales, los Estados Partes garantizarán, en particular: ... vii) Que se respetará plenamente su vida privada en todas las fases del procedimiento...".[31]

9.- Protección de datos personales

El régimen de protección de los datos personales establecido por la ley 25.326 -también llamada ley de "hábeas data"- y reglamentado por el decreto 1558/2001, basado en el derecho reconocido por el artículo 43 de la Constitución Nacional, permite que los ciudadanos ejerzan un legítimo poder de disposición y control sobre sus datos personales.

A tal fin, los faculta a decidir cuales de esos datos quieren proporcionar a terceros -sea el Estado o un particular- o que datos pueden esos terceros recabar, permitiendo asimismo que sepan quién posee sus datos personales y para que, pudiendo inclusive oponerse a esa posesión o uso.

Este poder de disposición y control sobre los datos personales se concreta jurídicamente en la facultad de consentir la recolección, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como sus posibles usos, ya sea por parte del mismo Estado o de un particular.

Y ese derecho a consentir o no el conocimiento y tratamiento -informático o no- de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quien dispone de esos datos personales y a que uso los está sometiendo, y por otro lado, el poder oponerse a esa posesión y a esos usos.

La citada ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

Como se ve, el derecho que se trata de proteger no es solo la intimidad, sino algo con mayor profundidad que en el derecho anglosajón se denomina "privacy" y que se ha castellanizado como "privacidad".

El objetivo es proteger aspectos de la personalidad que individualmente no tienen mayor trascendencia pero que, al unirse con otros, pueden configurar un perfil determinado de las personas. Ante dicha posibilidad surge el derecho de sus titulares a exigir que los datos permanezcan en el ámbito de su privacidad.

Capítulo II

BASES DE DATOS

SUMARIO: 1. Introducción; 2. Concepto; 3. Tipos de bases de datos; 3.1. Bases de datos estáticas; 3.2. Bases de datos dinámicas; 4. El derecho personalísimo sobre los datos personales; 5. Los registros del dato personal; 6. La informática y su utilización registral; 7. Averiguación de datos en Argentina; 8. La Dirección Nacional de Protección de Datos Personales; 9. Las defensas en protección del derecho personalísimo sobre los datos personales; 10. Bases de datos alcanzadas por la ley 25.326 y su decreto reglamentario; 11. Procedimiento de inscripción de las bases de datos; 12. Regulación de datos sensibles; 12.1. Recolección de datos sensibles; 12.2. Los datos sensibles y la disociación de datos; 13. La protección de datos personales y los informes crediticios; 13.1. Naturaleza del informe de riesgo crediticio; 14. Los archivos, registros o bancos de datos públicos; 14.1. Exigencias propias de los bancos públicos de datos; 15. Previsiones sobre el destino y destrucción de los datos; 16. Archivos, registros o bancos de datos privados.-

1.- Introducción

En la actualidad, y gracias al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos cuentan con un formato electrónico, lo que ofrece un amplio rango de soluciones al problema de almacenar datos.

En el presente capítulo nos propondremos desarrollar todo lo referido a bases de datos, relacionándolo con las nuevas tecnologías que el mundo de hoy ofrece y su impacto en la recopilación de información.

Vamos a enfatizar en los avances que la informática, sobre todo de la mano de Internet, produjo en este campo, pero también remarcaremos los problemas que están apareciendo en torno a este tema y los que pueden llegar a asomar próximamente si no se adoptan prudentes medidas.

2.- Concepto

Una base o banco de datos es un conjunto de datos almacenados sistemáticamente para su posterior uso.[32] En este sentido, una biblioteca puede considerarse una base de datos, compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

Internet en sí misma es una base de datos. Es considerada la "madre" de las bases de datos o la "gran" base de datos, por su capacidad de almacenamiento global y sin fronteras.[33]

3.- Tipos de bases de datos

Las bases de datos pueden clasificarse en dos grandes grupos:

3.1.- Bases de datos estáticas

Éstas son bases de datos de sólo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.[34]

3.2.- Bases de datos dinámicas

Éstas son bases de datos donde la información almacenada se modifica con el tiempo, permitiendo operaciones como actualización y adición de datos, además de las operaciones fundamentales de consulta.[35]

4.- El derecho personalísimo sobre los datos personales

Se ha dicho que lo que se protege a través de las acciones preventivas o correctores de las registraciones informáticas es el derecho a la identidad.[36] O, en todo caso que lo protegido es el derecho a la intimidad. También se ha propiciado considerar el bien del honor.[37]

En torno a lo que tiene que ver específicamente con los datos personales, se puede expresar que los mismos consisten en información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.[38]

El factor que se ve vulnerado al atacar la intimidad es la dignidad de la persona, fundamento último de todos los derechos personalísimos. La captación registral informática desnuda la personalidad en sus aspectos más salientes y recónditos.

A partir del entrecruzamiento de los datos puede accederse a la completa personalidad virtual, abarcando todos los bienes de la persona de una sola y única vez: intimidad, identidad, imagen, honor, cuerpo, salud, libertad y patrimonio.

La intimidad tiene su centro de atención en el conocimiento de los otros de aspectos privados de la persona. Consiste en un deseo de la persona a ser dejado solo, un deseo a sustraerse a la publicidad no querida. Los datos personales pueden ser destinados a registración publicística -Registro de la Propiedad, Registros Civiles, etc.-

Éstos no se proporcionan para su reserva total, sino para publicitarlos, aunque con ciertos límites, a los fines de evitar toda posible vulneración o violación.[39] En muchos casos, por cierto, a través del registro de datos se viola la intimidad, ya que la manipulación de esos archivos sirve de ataque a la vida privada.[40]

5.- Los registros del dato personal

A partir de la escritura, el ser humano preservó el recuerdo de los hechos con mayor seguridad. Aprovechó esa técnica expresiva para perpetuar historias, comunicaciones y datos.

Aquello que antes se almacenaba en la memoria del ser humano y se transmitía oralmente, pudo permanecer con mayor certeza y facilidad en los papiros y palimpsestos.

La imprenta abrió la gran puerta hacia la comunicación sin fronteras y, al mismo tiempo, facilitó el acumulamiento y guarda de las descripciones, de los conocimientos y de las narraciones.[41]

Cuando los datos centraron su objeto en la persona se formaron los archivos y registros de papel, que acumularon todo en cuanto al hombre se refería, desde el nacimiento hasta mucho más allá de su muerte, desde lo puramente material hasta lo patrimonial. Esto hacía que tanto el archivo de información como la posibilidad de supresión de la misma fuese lenta y tediosa.[42]

6.- La informática y su utilización registral

La informática no ha agregado nada nuevo a la operación de acopiar la historia personal y patrimonial de cada individuo. Constituye algo así como un instrumento perfeccionado en el cual se pasó del soporte de cartón, papel, fichas, libros, cuadernos, hojas, películas, fotocopiado y cintas, a la memoria de los ordenadores computarizados en donde se incorporan, relacionan y duermen ahora los datos, o bien reviven instantáneamente a voluntad de quien opere con ellos.[43]

La informática posee y plantea hoy en día múltiples posibilidades que nos parece oportuno detallar a continuación:

a) La rapidez en el archivo y formación de datos;
b) La casi instantánea transmisión de esos datos;
c) El almacenamiento total y en un espacio muy reducido;
d) La posibilidad de cubrir los tres tiempos de toda persona: el pasado, el presente y el futuro;
e) La perpetuidad de los registros, que pueden permanecer inalterables;
f) La búsqueda y el encuentro casi instantáneo de los resultados;
g) La modificación y el borrado de datos sin dejar rastros.[44]

Con dichas posibilidades operativas, estos son algunos de los peligros que se plantean para con los derechos de las personas:

a) El asentamiento de datos en instituciones no destinadas a recabarlos -como el caso de los llamados "datos sensibles", es decir, aquellos referidos a: religión, raza, ideología, política, opiniones, tendencias psicológicas, conformación física, hábitos, vicios, prácticas deportivas, relaciones sexuales, situaciones familiares y parentales, etc-;
b) Registrar datos sin la autorización de la persona registrada;
c) Impedir que la persona tome conocimiento de los datos que le conciernen;
d) Mantener en los registros datos innecesarios por haberse agotado la finalidad de su asiento, el plazo establecido o la voluntad del sujeto en conservarlos;
e) Aprovecharlos con fines diferentes al apropiado y a los que motivaron la compilación;

f) La difusión masiva incontrolada de éstos;
g) El cúmulo de cuestiones que corren el peligro de ser comunicadas al universo por vía de Internet.[45]

7.- Averiguación de datos en Argentina

Lo que a continuación vamos a compartir pareciera ser una información casi con matices de ciencia ficción, pero lo cierto es que navegando por Internet y sin violar ningún acceso se puede conocer información gratuita y pública de los argentinos con sólo ingresar su CUIL (Código Único de Identificación Laboral) o CUIT (Código Único de Identificación Tributaria). De esta manera se puede conocer, por ejemplo, el estado financiero de cualquier persona.[46]

Además, en Internet se puede tener acceso a todo tipo de información acerca de la fecha de nacimiento de una persona, su nombre, impuestos pagos o impagos.

También respecto a la propiedad de automóviles, historia laboral, obra social, seguridad social, teléfono fijo, etc, solamente partiendo del DNI (Documento Nacional de Identidad).[47]

Esto demuestra a las claras que nuestro país -a pesar de contar con una moderna normativa-, en asuntos de seguridad en el tratamiento de datos personales -sobre todo en lo que a Internet respecta-, tiene mucho trabajo por delante.

La mayoría de nosotros, alguna vez, hemos completado con nuestros datos personales cupones para participar de cualquier tipo de sorteo o promoción. Lo cierto es que algo que parece una práctica tan segura e inocente sirve para incrementar y enriquecer múltiples bases de datos, lo que potencia que éstas luego se transfieran onerosamente, cambien de dominio, y que nuestros datos viajen dispersos y sin control por la red.[48]

8.- La Dirección Nacional de Protección de Datos Personales

La Dirección Nacional de Protección de Datos Personales -DNPDP- es el órgano de control creado en el ámbito Nacional para la efectiva protección de los datos personales. Tiene a su cargo el Registro de las Bases de Datos, instrumento organizado con el fin de conocer y controlar las bases de datos.

Asesora y asiste a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos.

En este sentido, tiene por función investigar si la base de datos denunciada da cumplimiento o no a los principios que establece la ley y las disposiciones reglamentarias. La Dirección Nacional de Protección de Datos Personales informará acerca de:

1. La existencia de una base de datos.
2. Para qué obtiene los datos esa base y cuál es su fin último.
3. El nombre y domicilio del responsable de la base de datos.[49]

En caso que una base de datos no cumpla con los requisitos que establece la ley para la protección de sus datos personales, el titular podrá ejercer las siguientes acciones:

a) *Denunciar el hecho ante la DNPDP*

En caso de comprobarse el hecho denunciado, podrá aplicar sanciones administrativas al registro, archivo, base o banco de datos.(Ley Nº 25.326 art. 31[50]).

Es importante destacar que las denuncias que se hagan ante la DNPDP, son al exclusivo efecto de revelar deficiencias o incumplimientos a las normas aplicables en el tratamiento de los datos personales que hagan los archivos,

registros bancos o bases de datos. Ello ayudará a que la DNPDP, como organismo de control de los registros, archivos, bases o bancos de datos, verifique el cumplimiento de los derechos consagrados en la ley.

b) Acción Judicial de Hábeas Data (Ley Nº 25.326 , Título VII)

Esta acción procede para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquellos. En caso de falsedad o discriminación, para solicitar la supresión, rectificación, confidencialidad o actualización de sus datos (art. 33).[51]

La DNPDP además ha lanzado la Red Argentina de Protección de Datos Personales (RAPDP) invitando a participar a todas las provincias argentinas, a fin de garantizar la protección integral de los datos personales.

Esta red consiste en proponer un sistema de estructuras administrativas provinciales ideado para asegurar de la protección de los datos personales en todo el territorio Nacional.

Cada estructura se desempeñará como nodo de Red independiente y serán creadas según el criterio de cada provincia, trabajando en conjunto con la Dirección Nacional de Protección de Datos Personales.

El principal objetivo de la Red Argentina de Protección de Datos Personales es el de garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, conforme lo establecido por la Constitución Argentina en su art. 43, párrafo tercero.[52] Tendrá los siguientes objetivos:

a) Hacer cumplir la legislación sobre protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso y rectificación de los datos personales.

b) Informar a los ciudadanos de todo el país acerca de los derechos en materia de protección de datos personales, y también de los procedimientos de reclamo que existan para su protección y defensa.

c) Vincular a las unidades provinciales (llamados nodos) con la Dirección Nacional de Protección de Datos Personales, desarrollando acciones conjuntas en materia de registración de bases de datos, capacitación de recursos humanos, inspecciones y relevamientos a nivel provincial y nacional.

Para el establecimiento de esta Red, la DNPDP está dispuesta a invitar a las Provincias a adherir al contenido de la Ley Nº 25.326 y su Decreto Reglamentario Nº 1558/2001.

Las provincias se encontrarán en condiciones de incorporarse a la Red, una vez conformadas las estructuras provinciales de protección de datos personales, mediante un Convenio entre las Provincias y el Ministerio de Justicia de la Nación.

La Red Argentina de Protección de Datos Personales permitirá a los diferentes sectores de la población acudir a la estructura provincial (nodo) para solicitar y obtener información de sus datos personales incluidos en los archivos, registros, bases o bancos de datos locales o provinciales.

Además el registro que se lleve a tal efecto será de consulta pública y gratuita, y se podrá rectificar, actualizar y suprimir o someter a confidencialidad los datos de los que sea titular el ciudadano, derechos que podrá ejercer sin cargo alguno, así como realizar denuncias y reclamos en relación al tratamiento de sus datos personales.[53]

La Red Argentina, por concepción, resulta para el Estado Nacional una herramienta eficaz para asegurar el correcto tratamiento y protección de los datos personales en todo el territorio de la República.

La DNPDP cuenta con la colaboración de la Subsecretaría de Defensa del Consumidor de la Nación. El 10 de noviembre de 2005 se han suscripto sendas Cartas de Intención

entre la Subsecretaria de Defensa del Consumidor de la Nación y la Dirección Nacional de Protección de Datos Personales para la colaboración en materia de defensa del consumidor y protección de datos personales.

De esta manera se aprovecha la extensa red de organismos de defensa del consumidor para recibir denuncias relativas a la protección de datos personales que son remitidas para el conocimiento de la DNPDP, incrementando el alcance efectivo a todo el territorio nacional.[54]

Es importante destacar que conforme a la adecuación de la normativa argentina de protección de datos a los postulados de la Directiva 95/46 de la Unión Europea, establecida mediante la Decisión de la Comisión Europea del 30/06/03, la Dirección Nacional de Protección de Datos Personales debe procurar extender en forma efectiva su actuación a todo el territorio de la República.

9.- Las defensas en protección del derecho personalísimo sobre los datos personales

Multiplicadas y no taxativas son las facultades que se desprenden de un minucioso análisis del artículo 43 de nuestra Constitución Nacional y que posee la persona o titular de los datos -entendiéndose por tal toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos personales sean objeto de tratamiento por parte de terceros- para reaccionar y defenderse frente a la manipulación y violación de su derecho a los datos personales.[55]

Ante esta situación todo sujeto podría exigir rápidamente que:

- Se le dé conocimiento de la información guardada por la entidad recolectora;
- Se la corrija si tiene errores;
- Se la actualice si figura con antecedentes históricos no correspondientes a la personalidad del presente;
- Se la suprima y haga cesar si ya no tiene sentido preservarla en la base de datos;

- Se impida su publicación y se la mantenga en reserva, salvo el caso de ciertos archivos que por intereses públicos y de terceros tienen que subsistir con los resguardos del caso (exigencia, por ejemplo, de un interés jurídico actual para conocerlos);
- Que haya un verdadero interés social para la recolección;
- Tratándose de datos confidenciales y sensibles, limitar al mínimo indispensable la incorporación a los registros;
- Reclamar y hacer cesar la obtención de datos por medios ilícitos o ilegítimos;
- Exigir el anonimato, cuando los fines son puramente estadísticos o de índole similar;
- Que se pueda identificar al agente que recolecta los datos.[56]

Lo que caracteriza a estas facultades de defensa puede ser resumido en dos conceptos principales: el control y el rescate. Es que el titular, aún habiendo entregado él al recopilador sus datos, puede mantener esas dos defensas, porque al ser un derecho personalísimo, jamás habrá de desprenderse *in totum* y radicalmente del mismo.[57]

Al ser el dato personal un elemento muy privado de cada individuo, es necesario que se mantengan las facultades de supervisión por quien dispone en alguna medida de sus datos.

El control representa la facultad de revisar periódicamente los datos propios, no sólo para vigilar su autenticidad, sino para ordenar la remoción, el traslado o transferencia y la actualización de los mismos.[58]

10.- Bases de datos alcanzadas por la ley 25.326 y su decreto reglamentario

El presente tema está regulado en los artículos 1º y 2º de la ley 25.326 y en el artículo 1º del decreto 1558/2001. La definición de lo que debe considerarse "dato personal" y de los sistemas de información alcanzados por la ley se encuentra en el art. 2° ("Definiciones"), donde expresa que a los fines de la ley se

entiende por “datos personales” a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables, y por “archivo, registro, base o banco de datos” indistintamente 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.[59]

El art. 1° se encarga de fijar los objetivos de la ley, y en su primer párrafo indica que la tutela legal está dirigida a los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, y en el tercero que en ningún caso se podrán afectar las base de datos ni las fuentes de información periodísticas.[60]

En su versión original la fórmula difería, por cuanto rezaba: *"los datos de carácter personal asentados en archivos, registros o bancos de datos, u otros medios técnicos de tratamiento de datos, electrónicos o manuales",* y no contenía alusión alguna a las bases de datos ni a las fuentes de información periodística.

11.- Procedimiento de inscripción de las bases de datos

El mismo se inicia completando el Formulario FA.01 de Inscripción, al que se accede por el sitio de Internet de la Dirección Nacional de Protección de Datos Personales[61]seleccionando la opción "Formulario de Inscripción".

Al iniciarse el trámite se asigna una clave confidencial de acceso personalizado al sistema que permite acceder para realizar cualquier trámite del Registro Nacional.

Una vez completado el formulario se debe entregar en la Dirección Nacional de Protección de Datos Personales la "Nota de Solicitud de Inscripción", completada en todos su campos y suscripta por el responsable de la base de datos, o por el apoderado o representante legal, según corresponda, con firma certificada por escribano público o entidad bancaria, a la que se deberán adjuntar las hojas impresas del Formulario FA.01, todas firmadas por el responsable.

El sistema expide una boleta que debe ser cancelada por los medios de pago habilitados y que se adjunta a la Solicitud de Inscripción.[62]

La Dirección Nacional de Protección de Datos Personales verificará el contenido, y si se detectaren errores u observaciones, se notifica al responsable para su corrección.

De no ser así, elabora el "Certificado de Inscripción", asignándole un número de Registro. Uno de los ejemplares queda a disposición del responsable y el otro se archiva en la Dirección Nacional de Protección de Datos Personales.[63]

A fin de fomentar las inscripciones y de facilitar el control popular respecto del cumplimiento del deber de inscripción, dicha entidad otorga a todo aquel que se registre la posibilidad de colocar en su página de Internet un isologotipo especial que permite al usuario conocer que la base de datos está inscripta, lo que puede otorgarle además una importante ventaja competitiva respecto de las "bases de datos clandestinas".[64]

En cuanto a la forma de inscripción, tanto en el caso de las bases públicas como en el de las privadas, es similar. Las bases privadas, además de la inscripción inicial, deben hacer inscripciones sucesivas.

Una fija, que implica la renovación anual de la inicial -que debe hacerse desde los cuarenta y cinco días corridos anteriores a la fecha de vencimiento de la inscripción- y otra en cualquier momento en que se produzcan modificaciones en los tratamientos.[65]

La inscripción se hace, como ya remarcamos, por una doble vía sucesiva: electrónica y física, y utilizando un formulario denominado en el Formulario FA.01 de “Inscripción de Archivos, Registros, Bases o Bancos de Datos Privados".

Una vez inscripta la base de datos electrónicamente, el trámite finaliza con el previo pago del valor del formulario de inscripción que no tiene costo cuando

quien se inscriba no explote comercialmente sus bases y la información que contenga el sistema refiera a menos de 5.000 personas.

Si se da sólo el primer supuesto, se debe abonar $150.-, e idéntica suma corresponde abonar por la inscripción de quienes presten servicios de tratamiento de datos personales por cuenta de terceros -art. 25, ap. 1° de la ley 25.326.[66]

A partir de allí, la tasa asciende a $300.- para todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes -artículo 21 ap. 1° de la ley 25.326-.[66]

En cuanto a los archivos, registros o bancos de datos con fines de publicidad, las Cámaras, Federaciones y Colegios Profesionales del sector privado, deberán abonar $300.- en carácter de validación anual de adhesión.

Toda renovación anual tiene un costo idéntico al de la inscripción, y todas las tasas de inscripción tienen un recargo adicional por cada 10.000 personas registradas, aunque si se trata de datos sensibles, el recargo es cada 1.000 personas.[67]

12.- Regulación de datos sensibles

Las bases de datos pueden contener datos ordinarios o datos sensibles. La diferenciación entre unos y otros se produce cuando se plantea algún tipo de discriminación personal basada, por ejemplo, en el origen racial o étnico, las opiniones políticas, etc. (ley 25.326, art. 7[68]).

Así, existen datos que en un principio pueden ser considerados ordinarios o normales y que pueden verse transformados en datos sensibles si a través del uso que de ellos se hace se generan formas de discriminación a sus titulares.

En primer lugar, nos parece oportuno realizar una consideración sobre los "datos sensibles" o "datos especialmente protegidos", esbozando que se trata de aquellos 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.[69]

Algunos autores consideran que la enumeración formulada en esta definición es taxativa. Otros, que se trata de un listado meramente enunciativo.

Quienes entienden que se trata de una enumeración taxativa señalan que ello no significa que los datos personales íntimos no tengan también protección legal. Todo dato que pueda generar por su contenido actitudes o conductas discriminatorias tiene la protección legal dentro del régimen general de protección de datos.[70]

Por su parte, los que entienden que se trata de un listado enunciativo señalan que inicialmente se atribuyó la calificación de "sensible" a la información vinculada con aspectos íntimos de la persona,[71] partiendo de la premisa de que el derecho a la protección de los datos personales implica la salvaguarda de los derechos al honor y la intimidad del titular del dato.[72]

12.1.- Recolección de datos sensibles

Una cuestión básica a considerar es la relativa a la recolección de los datos sensibles. En todos aquellos casos en que el tratamiento de este tipo de datos se encuentra autorizado se aplicarán, a los fines de su recolección, los mismos principios que rigen la recolección de datos en general, sin perjuicio de resaltar que, conforme con lo establecido en el art. 7, inc. 1° de la ley 25.326, la regla es que ninguna persona está obligada a proporcionar datos sensibles.

Con esta aclaración, vale expresar que en todos los casos deberá informarse al titular en forma clara y expresa sobre la finalidad para la que los datos serán utilizados y sus destinatarios; la existencia del banco de datos, su domicilio y responsable; el carácter obligatorio o facultativo de las respuestas; las consecuencias de proporcionar o no los datos y la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión (ley 25.326, art. 6[73]).

La información relativa al carácter obligatorio o facultativo de las respuestas y a las consecuencias de proporcionar o no los datos deberá ser más cuidadosa en el caso de los datos sensibles, ya que se le deberá hacer saber al interesado -como ya expresamos- que no está obligado a proporcionar tal tipo de datos. En este caso, se deben tener en cuenta consideraciones que hacen a la calidad de los datos y al impacto sobre las personas.

Relacionado estrechamente con lo expresado precedentemente, se encuentra el principio de calidad de los datos, establecido en el art. 4^{74} de la citada ley, según el cual los datos recolectados deben ser adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para la que fueron recogidos.

Del mismo modo, se requiere que la obtención no pueda hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la mencionada normativa, ni puedan utilizarse los datos para finalidades distintas o incompatibles con las que motivaron su obtención.

Se exige que los datos sean exactos y puedan actualizarse en caso contrario, así como también que se almacenen de modo que el titular pueda ejercer el derecho de acceso y que sean destruidos cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recolectados.

Esto significa que la recolección de los datos debe responder a una finalidad o propósito predeterminado, que se identificará con el interés legítimo de quien los recaba para su tratamiento, propósito que no puede ser modificado sin contar con un nuevo consentimiento del interesado.

Dicho parámetro rige todas las operaciones de tratamiento de datos desde su creación, pasando por su procesamiento y transferencia, hasta llegar a su supresión.

12.2.- Los datos sensibles y la disociación de datos

Conforme con lo dispuesto en la ley 25.326 -art. 7-[75], los datos sensibles y entre ellos, los relativos a la salud, pueden ser objeto de tratamiento con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Este proceso se conoce como disociación de datos, la ley la define como todo tratamiento de datos personales efectuado de manera que la información obtenida no pueda asociarse a persona determinada o determinable (ley 25.326, art. 2[76]).

Por su parte, al regular la cesión de datos se exige para hacer posible la misma que los datos sean cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, consentimiento que no será necesario cuando existan razones de salud pública, de emergencia o se trate de la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares mediante mecanismos de disociación adecuados (ley 25.326, art. 11[77]).

En materia de transferencia internacional de datos personales, en la que rige como principio general su prohibición cuando se la efectúe a países u organismos internacionales o supranacionales que no proporcionen niveles adecuados de protección, dicho impedimento legal no existe en lo que aquí nos interesa, es decir, para el intercambio de datos sensibles, en el caso de que así lo exija el tratamiento del afectado o tratándose de epidemias, en tanto y en cuanto se apliquen procedimientos de disociación.

También se dispone que las normas de la ley 25.326 no se aplicarán, entre otros casos, a las encuestas de opinión -que en algunos supuestos podrían revelar inclinaciones o preferencias políticas, religiosas, filosóficas y morales- y a las investigaciones científicas o médicas, en la medida en que los datos recogidos no puedan atribuirse a una persona determinada o determinable (art. 28[78]).

Ello significa que si la información se encuentra disociada, estamos frente a un dato anónimo, que por ende no goza de protección alguna.

En sentido contrario, toda vez que no puedan aplicarse procedimientos de disociación, procederá la protección legal contenida en los preceptos de la ley 25.326, sus normas reglamentarias y complementarias.

13.- La protección de datos personales y los informes crediticios

Una de las características peculiares del informe crediticio es su potencialidad de dañar derechos de las personas, en especial aquellos derechos cuyo correcto o pleno ejercicio depende de la información personal.

No obstante, existe un justificativo social -interés público- en la prestación de servicios de informes crediticios que los habilita, y es que constituyen una herramienta indispensable para el desarrollo del crédito, pues otorgan mayor certeza a la actividad financiera y bajan considerablemente los costos, beneficiando a toda la comunidad.

La actividad de informes crediticios en principio no afecta la privacidad de las personas, dado el carácter comercial de la información que utiliza, que no es información íntima, en especial cuando resulta alcanzada por un principio de publicidad por su trascendencia para un adecuado funcionamiento del mercado del crédito.

Con referencia a la información de juicios de contenido patrimonial, manifiesta la jurisprudencia que *"no vulnera principios de intimidad el informe dado por una organización que proporciona información a las entidades que lo requieran sobre posibles clientes, en tanto éstos se limitan a datos personales y juicios pendientes, no siendo ellos datos secretos ni confidenciales".*[79]

Reiterando en parte lo antes expresado, debemos esbozar que la protección de los datos personales y los informes crediticios tienen variadas y amplias relaciones. De hecho, la mayor presentación de acciones de hábeas data en los fueros judiciales es por vulneración o alteración de informes crediticios.[80]

En la actualidad, producir informes crediticios constituye una actividad industrial que provee una parte muy grande de la información personal, que es aquella vinculada con el crédito.[81]

Las relaciones de producción de la sociedad actual se miden en niveles de mayor o menor información con seguridad jurídica, que es la marca de confiabilidad de los negocios. Esa información influye poderosamente en cada actividad, produciendo como consecuencia directa un impacto certero en el corazón de cada operación económico-financiera.

Concretamente, no se trata de abstracciones, sino del componente más real del costo de los productos: el capital más el interés.[82] Las tasas de interés reflejan esas informaciones como un espejo.

Se trata de un círculo virtuoso donde más información significa menos riesgos y menos riesgos menores tasas de interés. La ecuación, por tanto, es simple: a mayor seguridad del negocio, menor costo.[83]

Es así, que los informes crediticios -o de riesgo crediticio- son, por un lado, una herramienta muy valiosa para el mundo de los negocios, y por el otro, una actividad de alta sensibilidad para la sociedad, sean comerciantes[84] o no, pues hoy en día es necesario un informe positivo para el desarrollo normal de una actividad económica, dado que opera como carta de "buen hombre de negocios" y es una llave de acceso al crédito.[85]

Ante tal realidad, el Derecho ha puesto su interés en analizar el tratamiento de datos personales que desarrollan las empresas de informes crediticios,[86]intentando extremar los recaudos para procurar que los datos sean exactos y veraces.[87]

A partir de la sanción de la ley 25.326 se ha realizado una amplia regulación del tratamiento de datos personales, posicionando al país -respecto a su normativa- entre los países más avanzados en la materia.[88]

13.1.- Naturaleza del informe de riesgo crediticio

El informe de riesgo crediticio está compuesto por datos identificatorios de las personas y "hechos" de carácter patrimonial relativos a la solvencia y al crédito.

Nos referimos a "hechos" por cuanto los informes de riesgo crediticio deben transmitir información objetiva, sin juicio de valor, a fin de cumplir con los principios de veracidad y certeza exigibles a esta actividad. Los juicios valorativos no son apropiados en esta clase de informes, ya que introducen opinión al momento de juzgar -información subjetiva-.

Si se admitieran juicios de valor nos enfrentaríamos a las siguientes posibles consecuencias:

a) Alta probabilidad de transmitir una información no cierta; y

b) Condicionamiento del receptor a actuar en base a tal juicio antepuesto, lo que aumenta el riesgo de ocasionar un daño en el patrimonio de quienes participen de dicho informe.[89]

La veracidad y la certeza son la finalidad última del informe de riesgo crediticio, buscando despejar la incertidumbre en las relaciones económicas. La incertidumbre es un disvalor que altera la transparencia de los mercados y dificulta el acceso al crédito.

Podemos decir que los preceptos de la figura bajo análisis están implícitamente insertos en la reforma del art. 42 de la Constitución Nacional del año 1994[90].

La veracidad exige que la información sea completa, evitando verdades parciales que tornen en inexacta o incierta a la información. Ahora bien, esta completitud de la información es exigible dentro de un marco de razonabilidad, procurando evitar exigencias que, por su rigor, resulten paralizantes de la actividad informativa.[91]

Otro aspecto a considerar es el carácter "patrimonial" de la información, la cual es un requisito sustancial de la calidad del dato. En el concepto patrimonial se incluye a toda información relevante para evaluar la solvencia económica y crediticia de las personas, siempre y cuando no afecte la intimidad del titular del dato o contravenga prohibiciones especiales -art. 4 de la ley 25.326[92]-.

Asimismo, estos informes deben desarrollarse dentro de un marco de difusión restringido o condicionado, en atención el riesgo que implica su tratamiento, que en términos de nuestra legislación de protección de datos personales consiste en el requisito previo del interés legítimo, exigible al cesionario, y definido por el art. 26 de la ley 25.326.[93]

14.- Los archivos, registros o bancos de datos públicos

El carácter de "públicos" proviene exclusivamente de la pertenencia de los registros a la organización estatal. El banco de datos público tiene elementos objetivos de naturaleza pública y finalidad también pública, por oposición al privado que se organiza y sostiene en la esfera privada y su finalidad puede ser sectorial o corporativa.

Nada tiene que ver la naturaleza del banco de datos con la capacidad de los particulares para acceder a la información que contienen. Dicho de otra forma: no es el carácter público de la información -concebido como la posibilidad de un acceso inmediato y simple a la misma- lo que da al banco naturaleza pública o privada.[94]

Estas bases, bancos o archivos, pueden tener registrados o almacenados tanto datos públicos, de acceso público irrestricto, o de fácil acceso, como datos sin esas características, entre estos últimos, informaciones obtenidas con el consentimiento de los titulares para su tratamiento sujeto a las condiciones de dicho consentimiento, o de tenor reservado, confidencial, e incluso, secreto.

O sea que el tenor o calidad de la información que tratan o almacenan resulta independiente de su carácter público, exclusivamente determinado por su pertenencia a la organización estatal.[95]

También, en relación a los bancos públicos de datos resulta intrascendente que se encuentren o no destinados a proveer informes, en tanto y en cuanto esta característica ha sido establecida tanto por la Constitución Nacional como por la ley 25.326, exclusivamente respecto de los bancos de datos privados.[96]

14.1.- Exigencias propias de los bancos públicos de datos

Con respecto a este tema, en primer lugar se requiere la indicación de las personas de las que se pretende obtener los datos, y el carácter obligatorio o facultativo del suministro de tales.

Esta indicación dará transparencia al archivo, permitiendo confrontar la exactitud de las finalidades declaradas de su formación, y, asimismo, permitirá conocer el grado de coerción informativa que se le pretende imprimir a la obtención de los datos que habrán de conformarlo.

Sólo puede asignarse carácter obligatorio al suministro de datos destinados a archivos públicos de datos, y siempre y cuando sus finalidades justifiquen la consagración de ese carácter.

Finalidades tales como la preservación de la salud pública, la defensa nacional, etc. -cuya tutela corresponde exclusivamente al Estado-, pueden dar lugar a la asignación de obligatoriedad al referido suministro.

La indicación de los órganos responsables del archivo y su dependencia jerárquica tiene por objeto la identificación precisa de los responsables concretos de los bancos de datos públicos, como igualmente la de sus superiores ante quienes eventualmente recurrir las decisiones de esos órganos.

En la extensa y diversificada estructura estatal este recaudo aparece como obviamente razonable.

Similares razones justifican la identificación de las oficinas concretas ante las que los titulares de los datos pueden ejercitar los derechos que les reconoce la ley de protección de datos personales (acceso, rectificación, etc.).

15.- Previsiones sobre el destino y destrucción de los datos

La ley, en el inc. 3º del artículo 22[97] establece que en las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Esta exigencia se encuentra orientada a poner en conocimiento general el destino final de los archivos y de los datos que contienen, cuando la organización estatal decide la supresión de los primeros.

Es que la supresión de una base o banco de datos puede implicar tanto su descomposición, con la consiguiente destrucción de la información registrada, como su incorporación o absorción por otro archivo creado o a crearse, como igualmente la cesión o transferencia total o parcial de datos a otros registros.

Estas circunstancias, conforme lo dispone la norma, deben ser establecidas para que pueda tenerse conocimiento del "destino" de las informaciones archivadas.

Si la supresión del archivo conlleva la destrucción de los datos, también deberá indicarse en la normativa que disponga esa supresión, los medios que habrán de utilizarse para ese procedimiento.

Asimismo, estas informaciones serán necesarias para los eventuales afectados que ejerciten los derechos reconocidos por la LPDP (por ejemplo, determinados datos personales obrantes en un archivo de acceso restringido, de suprimirse ese archivo y ser transferidas las informaciones a uno de acceso público irrestricto, podría justificar que los titulares exigieran el sometimiento a confidencialidad de esos datos).

16.- Archivos, registros o bancos de datos privados

El art. 24[98] impone a los particulares que formen archivos, registros o bancos de datos, su registración en los términos del ya comentado art. 21[99] de la ley, cuando tales ficheros no sean para un uso exclusivamente personal.

Interesa resaltar la terminante disposición contenida en el art. 24[100] que sólo excluye del registro -cuya obligatoriedad y condiciones prescribe en el art. 21- a los archivos de "uso exclusivamente personal".

La ley, sin duda, se ha hecho eco de la preocupación generada por las especiales características impresas por el progreso de la informática y las telecomunicaciones a la registración, procesamiento y comunicación de informaciones, y especialmente de datos de carácter personal, incluyendo en el alcance de sus previsiones a todos aquellos registros o archivos que -de un modo o de otro- escapan a la esfera de la utilización estrictamente personal de sus titulares.[101]

Los arts. 1º[102] y 21[103] de la reglamentación aprobada por dec. 1558/2001 ratificaron este criterio, conforme se ha analizado al comentar dichas disposiciones.

El destino de los datos almacenados en cualquier archivo o registro, dadas las posibilidades técnicas existentes, resulta hoy sin duda alguna, notoriamente incierto y de control extremadamente difícil.

La norma así diseñada permitirá, si bien en la mayor parte de las oportunidades de modo *ex post facto*, tanto al organismo de control como a los titulares de los datos, ejercitar sus facultades y derechos, ante operaciones de tratamiento de informaciones en contravención con las disposiciones de la ley de protección de datos personales.

Antes de la entrada en vigencia de la ley 25.326 la situación, obligaciones, deberes y facultades, tanto de los responsables de los archivos como de los titulares de los datos, se encontraban en un "cono de sombras", muchas veces

contradictoriamente aclarado en las diversas decisiones judiciales que se fueron dictando a consecuencia de la operatividad del instituto del "hábeas data" por su consagración en la reforma constitucional del año 1994.

La necesidad de reglamentar el precepto constitucional fue señalada reiteradamente por la doctrina, la que además se ocupó de criticar el estado de cosas generado por el crecimiento de la actividad de colección, almacenamiento, procesamiento y comunicación de datos personales, sin el imprescindible marco regulatorio.

Se expresó en este sentido que una operatoria desregulada como la actual y carente del más mínimo seguimiento o evolución de las circunstancias informadas constituye un verdadero caso de polución informativa al que debería aplicarse el principio de quien contamina paga que usualmente se prescribe para la contaminación ambiental.

Así, las empresas que hacen de la información un verdadero comercio -sin que ello resulte peyorativo- deben asumir todos los aspectos de su negocio y no sólo aquellos que resultan “rentables”.

En términos de información, la subsistencia en los bancos de datos carentes de vigencia y por ende de fidelidad, no son sino residuos contaminantes que dañan tanto a los demandantes de información cuanto a los “sujetos observados”.[104]

Desde una perspectiva similar también fue objeto de críticas el tratamiento dado por bancos o bases de datos de carácter privado a informaciones relativas a actuaciones judiciales, registradas, procesadas y comunicadas sin adoptarse los recaudos pertinentes en orden a la preservación de la calidad de los datos, su eventual carácter confidencial, su vigencia, etc.

Estas consideraciones, entre muchas otras de parecido tenor, resultaban indudablemente justificadas, y remarcaban la imperiosa necesidad del dictado de una legislación acorde con las exigencias de la situación generada.

Capítulo III

INTERNET Y LAS NUEVAS TECNOLOGÍAS

SUMARIO: 1. Introducción; 2. La Internet; 2.1. Concepto; 3. El impacto de las nuevas tecnologías en el Derecho; 4. Los comienzos de Internet; 5. Las “Cookies” y el “Spam” (y la violación de la privacidad y la intimidad); 5.1. Las “Cookies”; 5.2. Concepto; 5.3. Los "Hipoconsumidores Tecnológicos" y "Analfabetos funcionales (de Internet)"; 5.4. Constitución Nacional; 5.5. Ley 25.326 - Ley de Protección de Datos Personales; 5.6. El "Spam"; 5.6.1. Concepto; 5.6.2. La ilegalidad del "Spam"; 6. Jurisprudencia; 6.1. Primera sentencia que declaró como ilegal al spam en la República Argentina; 6.1.1. Introducción; 6.1.2. Resumen del fallo; 6.1.3. Resolución del fallo; 6.1.4. A modo de conclusión; 7. Internet y legislación; 8. Conclusiones sobre este capítulo.-

1.- Introducción

En el presente capítulo analizaremos en profundidad el fenómeno de las nuevas tecnologías y su impacto en el Derecho -principalmente de la mano de Internet-.

2.- La Internet

2.1.- Concepto

La Internet es una red mundial de computadoras u ordenadores. La expresión “red de redes” hace referencia a que está formada por la interconexión de otras redes menores. De aquí también que anteceda a la palabra un artículo femenino, haciendo referencia a “la red” (la mega red).

Aparece por primera vez en 1969, cuando se establece la primera conexión en Estados Unidos entre tres universidades de California y una en Utah.

3.- El impacto de las nuevas tecnologías en el Derecho

En este siglo la humanidad está incorporando, y continúa haciéndolo, recursos tecnológicos que se suman a la vasta gama de los ya existentes. Si bien es discutible afirmar que ante este hecho nos encontramos ante el nacimiento de una nueva "edad" de la Historia (a la cual se la ha llamado "tecnotrónica" -Z.Brzezinsky- "de la tercera ola" -A.Toffler- o "de la información" -J.Nassbitt-) es indudable que los indicadores de novedades son obvios e inequívocos.

Toynbee indicaba que la historia se está acelerando de tal modo que nos sorprende constantemente merced a los extraordinarios avances modernos.[105]Se puede estar a favor o en contra de estos avances.

Lo cierto es que se han producido transformaciones respecto a las cuales el Derecho no puede ser ajeno a éstas, y por ende debe ponerse al día. Esto no debe

implicar necesariamente aprobar siempre ni el cambio sin sentido, ni sus consecuencias sin adoptar una actitud valorativa.[106]

Una sofisticada tecnología -llamada internacionalmente “Alta Tecnología” ("High-Tech")- se presenta ante el Derecho, en muchos casos inmerso en las viejas instituciones legales, de las cuales parece no querer desprenderse.[107]

El Derecho debe ir mudándose, poco a poco, de las bibliotecas y de los libros, de los juzgados en oscuros edificios, del mundo de los contratos escritos y de los expedientes donde son archivados, a un mundo donde la información esté cada día en las pantallas de las computadoras.

Con esto nos referimos a la inminente necesidad de una masificación de la tecnología en los tribunales, a los fines de agilizar la operatividad y brindar una justicia más rápida y eficaz.[108]

Claro ejemplo del avance que se está experimentando es Internet -la llamada "autopista de la información"-[95] que alude a los recursos capaces de obtener máxima sinergia del empleo conjunto de la informática, el cable y las telecomunicaciones, de manera de permitir principalmente el acceso a una multitud de servicios, en un contexto que traspasa las fronteras.[109] Lo cierto es que con Internet estamos asistiendo a una "desmaterialización de los soportes".

Esto es que ya no importa donde se encuentran los datos, lo que le interesa al usuario es acceder a ellos de la forma más rápida, eficiente y económica posible. Se puede con ello afirmar que la computadora ha cambiado las nociones de tiempo, espacio y distancia.[110]

Internet “es una nueva forma de socialización”[111] que, desde su arribo, planteó una nueva problemática a estudiar que va más allá de los límites de un país o nación, ya que la "red" conforma en la actualidad otra de las formas globalizadoras de la vida de los hombres en el mundo de hoy.[112]

4.- Los comienzos de Internet

Internet tiene en su nacimiento un origen militar y su historia se remonta al temprano desarrollo de las redes de comunicación. La idea de una red entre ordenadores diseñada para permitir la comunicación general entre usuarios de varias computadoras se ha desarrollado en un gran número de pasos. La unión de todos estos desarrollos culminó con la "red de redes" que conocemos como Internet.[113]

Las más antiguas versiones de estas ideas aparecieron a finales de los años ´50. Implementaciones prácticas de estos conceptos empezaron a finales de los ´60 y a lo largo de los ´70. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo.

En los ´90 se introdujo la World Wide Web, cuya utilización desde aquel momento se volvió masiva. La infraestructura de Internet se esparció por todo el mundo para crear la moderna red mundial de ordenadores que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a información y comunicación sin precedentes, pero también una brecha digital en el acceso a esta nueva tecnología, cuestión que no debe ser pasada por alto.[114]

Con respecto al tamaño de la "red", en 1981 existían aproximadamente 300 servidores en línea. En 1989 ese número creció a 90.000 computadoras; y en 1993, a más de un millón. Hoy se calcula que el 60 % de los ordenadores conectados a la red están ubicados en Estados Unidos. Ya en 1999 se estimaba una cantidad de usuarios conectados en una cifra aproximada a los 200 millones. Estas cifras van en constante crecimiento en todo el mundo, alentadas en algunos lugares por el sostenido e incesante crecimiento económico.[115]

Refiriéndonos a la Argentina y al uso que hoy en día se le da a Internet, se debe expresar que las cifras van en aumento, producto de la masificación de la tecnología y de la posibilidad del acceso a ella a través de un costo cada vez más

razonable. A esto se suma también el crecimiento sostenido que experimenta la economía de nuestro país por estos días.[116]

Uno de los mayores usos que los internautas le dan a Internet es el envío de e-mails -correos electrónicos-, cuestión respecto a la cual cobra protagonismo el denominado "Spam", figura que será objeto de análisis y explicación a lo largo del presente capítulo.[117]

5.- Las "Cookies" y el "Spam" (y la violación de la privacidad y la intimidad)

Seguidamente, analizaremos la violación de la intimidad y la privacidad a través de los modernos bancos de datos, que se encuentran potenciados como consecuencia de Internet. Y dentro de este amplio panorama, nos abocaremos a dos cuestiones fundamentales: las "Cookies" y el "Spam".

5.1.- Las "Cookies"

5.2.- Concepto

Se entiende que las "Cookies" son "pequeños ficheros o archivos de datos que se generan a través de las instrucciones que los servidores web envían a los programas navegadores, y que se guardan en un directorio específico del ordenador del usuario"[118]. Son archivos de información que envían algunos sitios de Internet tomando información a través del browser del usuario (como por ejemplo los gustos que tiene, los datos personales, las páginas que visitó, etc.).

Son una excelente herramienta de marketing para los spammers. Consisten en un número que identifica unívocamente al usuario y que se utiliza como índice en una base de datos en la que se almacena toda la información recopilada. De esta forma, cada vez que un usuario se conecta, la cookie permite que el servidor lo reconozca y pueda continuar recabando información. Cada usuario que visita un web site deja un rastro o número IP de origen que permite comprobar qué sectores del mismo ha visitado.

Las cookies fueron originalmente diseñadas para facilitar que un web site pueda distinguir el navegador del usuario como visitante anterior, y de ese modo adecuar su contenido y prestaciones a las preferencias de navegación de quienes lo vuelven a visitar.

A través del tiempo su uso se ha convertido en un valioso instrumento de obtención de información para los departamentos de marketing y publicidad de las empresas que operan en Internet. Con la información recopilada pueden estudiarse los hábitos de consumo de un usuario, sus preferencias en la web, el tiempo dedicado a cada página, los sitios que ha visitado con anterioridad, los banners que ha visto, el número de transacciones efectuadas, qué páginas lee, qué fotos mira, qué programas descarga, qué productos le interesan y cualquier otra información.

Si no se las utiliza en forma apropiada, esta herramienta puede vulnerar el honor y la intimidad de las personas. Por ello, si una cookie recopila información al solo efecto de efectuar transacciones cliente-servidor, pero no la asocia con persona alguna, no vulnerará el derecho a la intimidad de los usuarios. Por el contrario, si los datos recopilados pueden vincularse a una persona determinada, el riesgo de violación de la intimidad es grande.

Por lo general, los web sites incluyen en sus “Políticas de Privacidad” un apartado especial tendiente a informarle al usuario acerca del uso de cookies. Allí se le explica que tiene la posibilidad de impedir su acceso mediante la opción correspondiente de su navegador y se le hace saber que, de no hacerlo, se supone que acepta su ingreso y la recopilación de datos personales habitualmente denominados "información no específica".

Lo cierto es que con esto no alcanza. Los web sites deben contar con una clara Política de Privacidad que le informe detalladamente a los usuarios cuáles son los datos personales que la cookie recopilará, que destino se le dará a esos datos y si se compartirán con terceros, para permitir una aceptación libre, expresa e informada. Además, en los supuestos de aceptación de una cookie, siempre se debe ofrecer al usuario que la recibe la posibilidad de solicitar en cualquier momento que sus datos personales sean excluidos de la base de datos en la que hayan sido incorporados.

El uso de "Cookies" es uno de los modos más evidentes de violación de la confidencialidad de los datos personales,[119] habida cuenta que generalmente sin nuestro conocimiento gran cantidad de información personal va a estar formando parte de grandes bancos de datos.[120] Además, esta situación se ve sustancialmente agravada cuando quien recolectó nuestros datos personales a través de las "cookies" luego los transfiere -vende, cede, comparte, etc- a terceras empresas. Incluso la intimidad puede ser violada no sólo a través de cookies ilegales, sino también en los casos de bancos de datos confeccionados de acuerdo a la ley, pero que no cuentan con las medidas de protección suficientes.

Y así, entonces, permiten que esos datos personales puedan ser obtenidos por terceras personas, como aconteció con "Terra.com" -subsidiaria de Telefónica-, cuando en el mes de agosto de 2001 permitió la "fuga" de datos de muchos de sus usuarios.[121]

5.3.- Los "Hipoconsumidores Tecnológicos" y "Analfabetos funcionales (de Internet)"

La gran mayoría de todos nosotros somos "hipoconsumidores tecnológicos" y "analfabetos funcionales" -de Internet-, dado que nuestros conocimientos específicos sobre la red son mínimos y se pueden asemejar al conocimiento que un niño de jardín de infantes puede tener respecto a cualquier otro aspecto de la vida.[122]

Vale hacer referencia dentro de este marco a lo que tiene que ver con los sistemas "Opt-in" y "Opt-out". Consideramos ampliamente violatorio de la privacidad el sistema conocido por "Opt-out", el cual consiste en presumir que uno ha prestado su consentimiento a las "Cookies" si no expresa que no las quiere o no las acepta.

De hecho, existen infinidades de sitios en Internet que determinan que si uno no quiere las "Cookies" tiene que manifestarlo expresamente, para que las mismas no funcionen recolectando nuestros datos. Por ello, el sistema de "Opt-out", es decir, el hecho que se nos diga que podemos quitar las "Cookies" (que la gran mayoría de los usuarios de Internet no sabe siquiera de qué se trata) y que

nos expliquen cómo se deben quitar (hecho técnico éste que para la mayoría de los usuarios es una “misión imposible”) es absoluta y completamente ilegal, dado que en la práctica, es de casi imposible compresión y realización.

En cambio, el sistema de "Opt-in" es más transparente y respetuoso de la intimidad y la privacidad, dado que significa que si uno quiere que las "Cookies" funcionen -y recolecten sus datos-, debe incorporarse de manera expresa y voluntaria. De hecho, las organizaciones protectoras de los usuarios y consumidores prefieren este sistema.

En los Estados Unidos ya se han iniciado demandas contra empresas de gran envergadura por haber violentado la privacidad de los datos personales a través de "Cookies".[123]

Sin perjuicio de ello, es menester informar que una de las instituciones que más viola la intimidad a través de las Cookies es la propia Administración del Gobierno de los Estados Unidos, ya que 64 organismos distintos obtienen información de los usuarios que navegan en sus páginas, sin pedir ningún tipo de autorización.[124]

5.4.- Constitución Nacional

El art. 19 de la Constitución Nacional es una de las bases para la protección de nuestra intimidad y acciones privadas.[125] Se entiende que cuando dicho artículo se refiere a las acciones privadas también incluye a los datos personales.

Por ello, para que cualquier tercero (v.gr. empresas de Internet que trabajan con "Cookies"), puedan pretender, en forma legal, recolectar, guardar y archivar nuestros "datos personales", necesariamente deberán contar con nuestro consentimiento expreso, preciso, voluntario y, obviamente, revocable.

5.5.- Ley 25.326 - Ley de Protección de Datos Personales

Esta ley establece ciertos derechos y prohibiciones con relación a este tópico tan importante. Así, determina que el objeto de la ley es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos...", tendiendo a garantizar "...la intimidad de las personas. (art. 1°, Ley 25.326). Luego agrega (art. 2), que se entiende por datos personales a la información de cualquier tipo de las personas físicas o de existencia ideal.

Por ello, como primera pauta de análisis tenemos que decir que, además de la Constitución Nacional, existe una norma expresa tendiente a proteger todos nuestros datos personales.

Respecto a la ilegalidad del sistema de "Opt-out", debemos recordar que el art. 5[126] de la citada ley determina que el tratamiento de datos personales es ilícito, cuando el titular no hubiera prestado su consentimiento libre, expreso e informado.[127]

Resulta una obviedad después de todo lo visto que las "Cookies", a través del sistema de "Opt-out", violan todas y cada una de las previsiones de la normativa de la Ley 25.326, dado que no existe consentimiento, y además, la normativa vigente exige bajo pena de considerarlo ilícito, que dicho consentimiento debe ser libre, expreso e informado y plasmado por escrito.

También puede considerarse que las "Cookies" violan el art. 4, Inc. 2°[128], de la Ley 25.326, cuando se establece que la recolección de datos no puede hacerse por medios desleales, ni de manera fraudulenta. Ninguno de estos requisitos son cumplidos por el sistema de "Opt-out", y es por ello que reiteramos que no caben dudas de que las "Cookies", a través del mismo, son absolutamente ilegales.

5.6.- El "Spam"

5.6.1.- Concepto

En general, la doctrina especializada se refiere al "Spam"[129] como la utilización de correo electrónico para el envío de publicidad no solicitada.[130] El Spam es la técnica de envío indiscriminado de e-mails a miles de usuarios que no pidieron recibirlos e integra el grupo de los llamados "abusos en el correo electrónico", pues su práctica trasciende los objetivos habituales del servicio y perjudica a proveedores y usuarios.

Si bien la práctica habitual consiste en el envío de correo comercial y publicitario, no son pocos los casos en que se lo utiliza con el fin de paralizar el servicio por saturación de las líneas, del espacio en disco o de la capacidad de procesamiento de un servidor.

En la mayoría de los casos el spammer -así se denomina a quienes practican esta actividad- es desconocido y la dirección de correo que aparece en el remitente es falsa, lo que impide identificar una dirección de retorno correcta para responder el mensaje.[131]

Constitutye una práctica que ha sido condenado desde los albores de Internet, pero lo cierto es que son pocas las voces que se alzan a favor de la prohibición total. Se ha convertido en un problema internacional que amenaza las comunicaciones y, para no ser menos, los argentinos ya estamos dentro de la lista de los países donde se originan la mayor cantidad de mensajes basura.

De hecho, se ubica a la Argentina en el quinto lugar en el mundo después de Estados Unidos, China, Corea del Sur y Brasil. Cada mensaje enviado por un spammer es transportado por varios sistemas hasta que llega al lugar de destino, generando costos a lo largo de la cadena.

El bolsillo de los usuarios es el que paga los pulsos de su cuenta telefónica por el tiempo que ocupan en descargar estos mensajes, además de los recursos de espacio de almacenamiento y tiempo para su lectura y eliminación. Por su parte,

los proveedores de servicio consumen ancho de banda para procesarlos y, por ende, la velocidad y calidad de sus servicios disminuye.

Finalmente, los costos se transfieren al usuario final, repercutiendo negativamente en la satisfacción de los clientes y en los ingresos económicos de las empresas. En la actualidad se calcula que el SPAM constituye poco más del 60 por ciento de los e-mails que circulan por Internet. Por eso, en todo el mundo se lo identifica como un peligro para las comunicaciones y varios países ya están castigando su uso.[132]

Se puede expresar que el problema de los "Spam" tiene, por lo menos, un triple análisis:

a) La pérdida de tiempo del usuario de Internet:

La catarata de "Spams" que se recibe en la casilla de correo electrónico[133] complica la tarea del usuario, dado que cuando se recepcionan decenas de mails no solicitados se pierde mucho tiempo abriendo cada uno de ellos. Ello es así, dado que necesariamente se debe hacer una “clasificación” de los distintos correos, para establecer cuáles eliminar y cuáles leer. La Comisión Europea, ha calculado que unos 500 Millones de "Spams" se envían diariamente y que su costo es de unos 9.300 millones de dólares al año en todo el mundo;

b) La violación de su intimidad:

Resulta claro que con los “Spams” se está conculcando la "privacidad", dado que el usuario de Internet se ve “invadido” por decenas de mails que no requirió, que lo “bombardean” con todo tipo de productos y/o servicios que jamás solicitó;

c) El conocimiento por parte del usuario que sus "datos personales" figuran en un "banco de datos ilegal":

Para que una simple publicidad sea depositada en la casilla de correo electrónico del usuario es necesario que previamente el emisor del mensaje sepa

cual es la dirección del mismo. Esto hace que se manipulen infinidades de bases de datos en la red, transfiriéndose a un tercero o a otra empresa. Ningún usuario tiene ni siquiera una leve idea de la cantidad de bases o bancos de datos en que puede estar figurando, al mismo tiempo, en toda la red.

5.6.2.- La ilegalildad del "Spam"

Todos los "Spams" se remiten a varios cientos o miles de personas. Y, las informaciones de los "correos electrónicos", necesariamente, surgen de una ″base de datos″. Es más, como es de público conocimiento, frecuentemente dentro de los "Spams" que recibimos nos llegan ofertas de "bases de datos" clasificadas por países, o provincias, o actividades, o profesiones, etc.

Es decir, más allá que el "Spam" en sí mismo esté prohibido o no, el hecho de enviarlos tiene un origen ilegal cuando para el envío de ese "correo no solicitado" se tuvieron que utilizar bases de datos obtenidas ilegalmente. En efecto, según se desprende de todo lo antes visto, existen muchas "bases de datos" que se confeccionan a través de métodos ilegales, dado que obtienen los "datos personales" (v.gr. e-mail del receptor del Spam), en abierta violación de la Ley 25.326.[134]

Así entonces, si existe una fortísima presunción "iuris tantum" que el sustrato en que se basa el "Spam" es ilegal, no existe otra alternativa que declarar la ilegalidad de todo aquello que deriva de una base de tal tipo. En el caso que quien envía el "Spam" sostenga que la "base de datos" tiene un origen legal, va a pesar sobre su propia cabeza la prueba de la legalidad de la misma.

Es pertinente recordar que el art. 27 de la Ley 25.326[135], prescribe que a los fines de la publicidad se podrán utilizar bases de datos cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

Por ello, tanto los datos que figuren en documentos accesibles al público, o que hayan sido dados por los propios titulares u obtenidos con su consentimiento,

necesariamente tienen que tener un origen legal, es decir, haber cumplido estrictamente con la Ley 25.326.

Y, obviamente, no sólo el origen de los datos tiene que ser "legal", sino que la persona que envía "Spams" tiene que comprobar y verificar que la base de datos que utiliza, ya sea propia o entregada por un tercero, cumple en forma puntual con la Ley de Protección de Datos Personales. De esta forma, quien recibe un “Spam” puede utilizar los procedimientos expresamente previstos en la Ley de Protección de Datos Personales (art. 33 y siguientes[136]), y exigirle al emisor del correo el origen, acceso y retiro de sus datos (art. 27, incisos 2° y 3°[137], de la Ley 25.326), bajo expreso apercibimiento de daños y perjuicios.

Por ello, no solamente es ilegal el envío de "Spams", sino que quien los remitió también va a resultar legalmente responsable, frente a todos los damnificados, dado que es partícipe en la difusión de los "datos personales" obtenidos antijurídicamente.

6.- Jurisprudencia

Habiendo infinidad de fallos respecto a los temas que son objeto de estudio y análisis en el presente trabajo -y en especial con respecto al hábeas data- hemos optado por abordar el que a nuestro entender constituye el más emblemático de todos, ya que se trata de la primera sentencia que declaró como ilegal el envío de spams en la República Argentina.

En la actualidad, esta cuestión se presenta como un desafío para el mundo del Derecho. Además se trata de una resolución actual, no solo por el tema al cual hace alusión, sino por la fecha cronológica en que se ha suscitado.

6.1.- Primera sentencia que declaró como ilegal al spam en la República Argentina

6.1.1.- Introducción

Este fallo plantea un nuevo e interesante sendero en el camino del Derecho hacia el análisis y la regulación de las nuevas tecnologías, procurando actualizarse a la par de los cambios que se van desarrollando en la rama de la informática.

Constituye un precedente por demás de importante en la jurisprudencia de nuestro país, demostrando -como ya lo hizo otras veces- que el Derecho es capaz de tornarse operativo aún cuando carece de las normas necesarias para ello -teniendo en cuenta que en la actualidad todavía carecemos de una ley que castigue el envío indiscriminado de publicidad a través del correo electrónico (spam)-.

La presente sentencia fue dictada por el Juzgado Nacional Civil y Comercial Federal N° 3, con fecha 7 de abril de 2006. Las partes intervinientes son: "Tanús, Gustavo D. y otro v. Cosa, Carlos A. y otro".[138]

6.1.2.- Resumen del fallo

Los Dres. Gustavo D. Tanús y Pablo A. Palazzi (letrados en causa propia), promovieron acción de hábeas data contra Carlos A. Cosa y Ana C. E. Magraner, con fundamento en el art. 43 CN y en la ley 25.326, a fin de obtener: a) el acceso a los datos personales de los actores, incluidos en las bases de datos que los demandados utilizan para enviarles mensajes de correo electrónico no solicitado (spam); b) la eliminación de esos registros en las mencionadas bases; c) el cese de todo tipo de tratamiento de dicha información; d) se condene a los demandados a adoptar los recaudos técnicos necesarios para proceder al bloqueo de toda dirección de correo electrónico vinculada con los actores.

Solicitaron y obtuvieron el dictado de una medida cautelar, tendiente a que los demandados se abstuvieren de enviar mensajes a las casillas de los actores así

como transferir o ceder a terceros la dirección de su correo electrónico u otro dato personal que se vincule a ellos.

Relatan que aquéllos, bajo el nombre de fantasía "Public soluciones informáticas", se dedican a la venta de bases de datos que contienen información personal de terceros, en especial de direcciones de correos electrónicos de millones de usuarios argentinos de Internet, cuya finalidad es hacer publicidad masiva e indiscriminada y para ello se valen precisamente del mismo método, es decir, el envío de correos electrónicos no solicitados, denominados spam.

Agregan también que promocionan sus servicios en diferentes sitios de Internet de los cuales se constató, son sus titulares. Explican que las bases de datos que comercializan los demandados -y que en reiteradas ocasiones les ofrecieron- no sólo contienen las direcciones de correo, sino también datos personales que, conforme a la ley 25.326 son considerados "sensibles" y que apuntan a diferenciar a los consumidores por perfiles o tipos.

Los actores destacan que en diversas oportunidades respondieron esos mensajes solicitando el cese de los envíos y el acceso a la información relacionada con ellos que los demandados tuvieran en su poder, así como también la eliminación de esa información de las mencionadas bases de datos.

Se explayan sobre la naturaleza del correo electrónico y del spam (envío de mensajes no solicitados) y resaltan que, a diferencia de la publicidad no requerida que se recibe habitualmente por otros medios como el correo postal, llamadas telefónicas o fax, en el caso del spam es el receptor quien asume parte del costo económico de esa actividad, ya que además del tiempo que se utiliza para "bajar" ese mensaje, implica un gasto por la conexión a cargo del usuario final, quien debe pagar el tiempo de tarifa telefónica y de servicio de Internet que conlleva ese proceso.

A ello, añaden el desgaste que se produce en el disco rígido de la computadora por la "fragmentación" (los espacios que quedan en el sistema) que se origina al borrar esos mensajes. Por último, destacan la invasión a la privacidad

que constituye este tipo de tratamiento de los datos personales, en violación a las disposiciones de los arts. 18[139] y 19[140] CN., 11 CADH[141] y 17 PIDCP[142].

Los demandados, con patrocinio letrado, solicitaron el rechazo de la acción por improcedente. Sostienen que no existe tal base de datos y que obtienen las direcciones de correo directamente de Internet.

Alegan que la actividad que realizan no puede calificarse como spam, dado que quienes envían este tipo de correos ocultan su identidad y ellos, por el contrario, se encuentran registrados como titulares de los dominios utilizados para la promoción del servicio.

Aducen que los pretensores dieron su dirección de correo electrónico personal en Internet, de modo que no pueden invocar que se haya infringido el art. 5 inc. 2[143] ley 25.326 cuando establece que no será necesario el consentimiento cuando los datos se obtengan de fuentes de acceso público irrestricto.

Finalmente, niegan comercializar datos "sensibles", así como también haber recibido por parte de los actores la solicitud del cese de envío de correos y que se les haya ocasionado a los demandantes un perjuicio económico.

A través del denominado "marketing de banco de datos" las empresas crearon un sistema por el que se brinda información gratuita vía personal, correo, telefónica o Internet a cambio de proporcionar datos personales que servirán a los fines de la publicidad de sus productos. Con esa información se configuran bancos de datos que contienen las características de los usuarios y que además se comercializan, quienes así comienzan a recibir gran cantidad de mensajes no solicitados en miras a concretar ventas.

Se produce entonces, un cruzamiento de datos que apunta a vender un determinado producto a quien compró otro con anterioridad y en razón de la información que dejó al hacerlo; esta situación se multiplica cuando tiene lugar a través de Internet, como consecuencia de la información que arroja el usuario en la red cuando ingresa a distintas páginas web, la cual es recolectada por las cookies y después es utilizada con una finalidad distinta de la que previó el mismo

cuando la brindó. Se desprende de la documental aportada por la actora que los demandados promocionan la venta, y hasta el obsequio, de bancos de datos.

A esta altura es preciso recordar la definición que brinda la ley 25.326 acerca del archivo, registro, base o banco de datos, cuando legisla que 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. (art. 2[144]).

A su vez, el decreto 1558/2001 reglamenta que quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquéllos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito (art. 1[145]).

El magistrado concluyó que la información que recolectan los demandados y el modo en que la organizan, o sea que agrupan las direcciones de correo electrónico por la profesión o actividad que desarrolla la persona, constituye incuestionablemente una verdadera base de datos, teniendo en cuenta también que en algunos casos el archivo que ofrecen a la venta incluye, también, datos como nombre y apellido, dirección, teléfono, fecha de nacimiento, número de documento e ingresos aproximados, o empresas con nombre, CUIT, cantidad de empleados, fax, responsable, cargo y rubro.

Igualmente ofertan la cesión o transferencia de los mencionados archivos a terceros, con la finalidad de enviar publicidad, y promocionan, además, un servicio que posibilita el envío de correos electrónicos ocultando la dirección remitente, en flagrante violación a lo dispuesto en el art. 6 inc. e y en el art. 14 de la ley, dado que ese accionar imposibilita o, por lo menos, dificulta el acceso a la base de datos.

Por otra parte, el tratamiento de los datos que los demandados llevan a cabo le adjudica a la información que tomaron de los actores un propósito distinto

del que ellos tuvieron en la oportunidad en que volcaron esos datos en Internet, en detrimento de lo dispuesto en el art. 4 inc. 3[146] de la citada ley.

Por otra parte, la ley 25.326 en su art. 27[147], permite el tratamiento de datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales, publicitarios, o que permitan establecer hábitos de consumo cuando éstos figuren en documentos accesibles al público (inc. 1).

No obstante, la norma prevé la posibilidad de que, en cualquier momento, el titular solicite el retiro o bloqueo de su nombre de los referidos bancos de datos (inc. 3). Así lo solicitaron los actores en reiteradas oportunidades a las direcciones de correo tarjetas@publicc.zzn.com y remover@publicc.com.ar -esta última arrojó un resultado negativo-. Tampoco obtuvieron resultado alguno cuando requirieron el acceso a los datos, puesto que con posterioridad a ello continuaron los envíos de mensajes.

Respecto del daño que los actores alegan que les originó la recepción del mentado correo masivo no solicitado, el juez entendió que el mismo existió, teniendo en cuenta el costo económico y el tiempo que esa actividad insume, además del tiempo de descarga que requiere identificarlos, seleccionarlos y borrarlos, el incremento en el costo de recepción y procesamiento, así como también la necesidad de implementar sistemas para bloquear y, aún lograr, la protección de los virus que pueden dispersar.

La pericia practicada da muestra del proceso de fragmentación que tiene lugar durante el almacenamiento y la eliminación de archivos y el perjuicio que ello ocasiona, que se traduce en una notable disminución de la velocidad de almacenamiento y obtención de información.

Asimismo, puntualiza que los correos electrónicos son archivos de pequeño tamaño y, consecuentemente, su excesiva grabación y borrado produce una mayor fragmentación del disco rígido de la computadora.

En estas condiciones, el magistrado entendió probados los extremos invocados por los actores en cuanto a la existencia de la base de datos, la inclusión

de sus datos personales, el envío masivo de mensajes con el consecuente daño que esa circunstancia provoca y el requerimiento de no enviar más publicidad a sus casillas de correo.

De este modo, además del daño apuntado precedentemente, la actividad de los demandados comporta una invasión en la esfera de la intimidad de los actores y de su tranquilidad, por cuanto se ven sometidos a la intromisión en sus datos personales que se ve reflejada en el envío masivo de mensajes no solicitados y la oferta de comercialización de esos datos que efectúan a terceros, cuando ya habían requerido el cese del envío y el bloqueo de esa información de la base respectiva, conforme lo previsto en el ya citado art. 27[148] de la ley 25.326.

Esta nueva faceta de la vida íntima de las personas -que se pone de manifiesto con el avance de las comunicaciones- merece el resguardo del ordenamiento jurídico, cuestión contemplada en el art. 1071 bis[149] del Código Civil.

Es importante destacar que la jurisprudencia extranjera ha sostenido que la garantía de la intimidad se traduce en un derecho de control sobre los datos relativos a la propia persona, siendo la libertad informática el derecho a controlar el uso de los mismos insertos en un programa informático, pudiendo el ciudadano oponerse a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.[150]

6.1.3.- Resolución del fallo

El juez resolvió hacer lugar a la acción de hábeas data promovida por los Dres. Gustavo D. Tanús y Pablo A. Palazzi y condenar a Carlos A. Cosa y a Ana C. E. Magraner para que en el plazo de diez días corridos:

a) permitan a los actores el acceso a los datos personales que poseen de ellos;
b) con posterioridad, los eliminen de las bases de datos que detentan;
c) cesen en el tratamiento de sus datos personales, con costas a su cargo.[151]

6.1.4.- A modo de conclusión

Según nuestro entender, y haciendo una breve conclusión sobre el fallo en cuestión, entendemos que la resolución a favor de la parte actora ha sido acertada, teniendo en cuenta que en el cuerpo de dicha sentencia se encontraron probadas todas y cada una de las pretensiones, siendo evidente el daño ocasionado al derecho a la intimidad como también así el daño patrimonial sobre el usuario/consumidor de Internet.

Debemos considerar que si bien puede suponerse que la vía judicial es la idónea para combatir el spam, no creemos que toda la solución pase por allí. Cierto es que el mundo entero se inclina por regularlo. Pero una ley local no impedirá que sigamos recibiendo inmensas cantidades de spams desde el exterior.

Es por ello que, además de un cuerpo normativo que establezca la forma en que pueden enviarse mensajes masivos de correo electrónico que no hayan sido solicitados previamente por el destinatario, es necesario que las empresas proveedoras de servicios de Internet y correo electrónico suscriban códigos éticos de conducta que las comprometan a impedir no sólo la recepción sino también el envío de spams a través de sus servidores.

También es recomendable que se castigue el desarrollo de software que permita enviar mensajes engañosos y que las empresas tomen conciencia de que enviar e-mails sin el consentimiento del receptor perjudica su imagen comercial.

Enviar infinitos mensajes de correo electrónico es tarea fácil para un spammer. Basta tener una cuenta de correo electrónico y una base de datos con direcciones electrónicas.

Aunque los spammers se excusan diciendo que el usuario puede defenderse borrando los mensajes recibidos o solicitando que su dirección se excluya de la lista de destinatarios, el problema es mucho mayor.

Cada mensaje enviado por un spammer es transportado por varios sistemas hasta que llega al lugar de destino, generando costos a lo largo de la cadena. El

bolsillo de los usuarios es el que paga los pulsos de su cuenta telefónica por el tiempo que ocupan en descargar estos mensajes, además de los recursos de espacio de almacenamiento y tiempo para su lectura y eliminación.[152]

Por su parte, los proveedores de servicio consumen ancho de banda para procesarlos y, por ende, la velocidad y calidad de sus servicios disminuye. Finalmente, los costos se transfieren al usuario final, repercutiendo negativamente en la satisfacción de los clientes y en los ingresos económicos de las empresas.

Mundialmente, gran parte de las propuestas legislativas existentes sobre la materia consideran apropiado el sistema de "Opt-Out", que permite a los usuarios solicitar que sus datos sean excluidos de las bases de datos utilizadas por los spammers para enviar sus ofertas comerciales.[153]

Uno de esos países es Estados Unidos, que desde hace tiempo viene demostrando interés en combatir este flagelo. Fueron varios los juicios que enfrentaron a gigantes de la industria de Internet contra empresas dedicadas a realizar campañas publicitarias a través del correo electrónico.[154]

Sin embargo, recién en diciembre de 2003 se ha sancionado una Ley Federal con alcance nacional. Europa eligió el camino inverso: La Directiva Europea se inclina por exigir que previamente el usuario se haya registrado voluntariamente para recibir mensajes, sistema conocido como "Opt-In".

En Argentina no hay aún una ley específica. Se conocen algunos proyectos, pero hasta el momento no han sido tratados por el Congreso. En el año 2001, en concordancia con las disposiciones de la Ley 25.326 de Protección de los Datos Personales, la Secretaría de Comunicaciones sometió a consulta pública un anteproyecto de ley especial sobre el tema basado en el sistema "Opt-Out".

Los programas utilizados para filtrar automáticamente los mensajes electrónicos no deseados son útiles, pero demostraron que solos no sirven para controlar el spam. Reducen la cantidad de mensajes, pero no son totalmente efectivos.

Hoy en día nos enfrentamos a datos e información digitalizada, con redes informáticas que traspasan o duplican la información en segundos, con un alcance mucho mayor que el que cualquier diario puede ofrecer.

Pero los fundamentos parecen ser los mismos, el acceso a la esfera privada del individuo, ya se trate de su propiedad, de su conciencia o de sus datos, requiere su consentimiento.

Si intentáramos clasificar y delinear cuáles son los ámbitos del derecho a la privacidad, podrían diferenciarse tres campos fundamentales.

El primero, es el campo de la privacidad espacial o la intimidad física, limitada a los ámbitos materiales donde el individuo se desenvuelve en forma habitual. Éste es el caso del art. 18 de la Constitución Nacional, que establece la inviolabilidad del domicilio y el secreto de la correspondencia epistolar.

También se extiende a la persona y al propio cuerpo y sus atributos, como la imagen, la voz, y demás derechos personalísimos relacionados. Incluye también el derecho a no ser molestado ni perturbado -en referencia al caso en cuestión- a través de spams.[155]

El segundo, es el campo del pensamiento y de la libertad de conciencia. El mejor reflejo de este ámbito es el art. 19 de la Constitución Nacional. Bajo este manto de protección constitucional el individuo tiene derecho a la libertad de pensamiento y de creencias, a la objeción de conciencia y, en definitiva, a tomar decisiones fundamentales sobre su propia vida, siempre que éstas no afecten al orden y a la moral pública, ni perjudiquen a un tercero.[156]

El tercer ámbito, es el campo del dato o de la información personal. En realidad, este campo siempre existió y fue uno de los que dio nacimiento al moderno concepto del derecho a la privacidad. Pero esta difusión de información personal se ha potenciado hoy día con la expansión del uso de ordenadores y redes informáticas.

Nadie puede negar que Internet posee un potencial de difusión masiva de información nunca antes alcanzado por otro medio de comunicación, debido en parte al increíble crecimiento que tuvo la red en los últimos años, pero también impulsado por la multiplicidad de datos y distintos formatos que soporta (textos, imágenes, videos pregrabados y en vivo, y sonidos).

Los tres ámbitos que hemos señalado están expresamente amparados por normas constitucionales. La línea divisoria que separa unos de otros es muy tenue, y a veces una situación puede caber en dos o más de ellos. Pero los tres están funcionalmente interrelacionados.[157]

Es decir, la privacidad espacial conduce a una privacidad del dato personal. A su vez, la privacidad de conciencia necesita de la posibilidad de preservar la información sobre la propia persona. La privacidad sobre la propia imagen puede ser violentada almacenando y tratando la imagen de una persona en ordenadores.[158]

7.- Internet y legislación

En la Argentina, el 23 de junio de 1997 se publicó en el Boletín Oficial el Decreto de Telecomunicaciones N° 554/97, declarando de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial Internet en condiciones sociales y geográficas equitativas, con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciones de la multimedia.

El mismo cuerpo normativo reconoce en parte las deficiencias estructurales de la Argentina en aquel momento para cubrir las expectativas de un país que se veía posicionado en el primer mundo, a la par de las grandes potencias. Dicho decreto intentaba no quedar al margen de uno de los avances más importantes en materia de comunicaciones que se conoce hasta el momento.

En nuestro país no existe un gran debate sobre la regulación de Internet ni demasiadas opiniones al respecto. En este marco de vacío es que cabe preguntarse si deberían dictarse nuevas leyes o si con las existentes el problema del avance de Internet estaría solucionado.

La gran duda es si una posible regulación carecería de aplicación práctica, por la propia naturaleza de la "red", ya que es técnicamente imposible controlar todo el material que desde distintas partes del mundo se vuelca en ella -dado que cualquier navegante se encuentra en condiciones de generar sus propias "señales" (sean estas imágenes, notas, etc.) y transmitirlas a quien sea y donde sea, en forma interactiva con otros usuarios-.

La "red de redes" se convierte así en una incógnita general, en referencia a su regulación, lo cual plantea un gran trabajo de análisis para el Derecho, en pos de no quedar al margen de la cuestión.[159]

8.- Conclusiones sobre este capítulo

Analizado el presente capítulo, creemos pertinente detallar los puntos más destacados que el mismo ha dejado. Es posible precisar las siguientes consideraciones:

- La violación de la intimidad y de la privacidad es una cuestión sobre la que debemos especial atención.
- Las "cookies", mediante el sistema de "opt-out", son ilegales.
- La gran mayoría de los usuarios de Internet son somos "hipoconsumidores tecnológicos" y "analfabetos funcionales".
- Los "datos personales" tienen amparo en la Constitución Nacional y en la Ley 25.326.
- La violación de la protección de los datos personales, se ve potenciada por el uso de Internet.
- Los "spams" que se sustentan técnicamente en bases de datos (obtenidas en violación de la normativa vigente), son ilegales.
- Quien envíe los ″spams″ tiene que probar que la base de datos que utilizó, tiene un origen lícito.
- Si no se acredita la legalidad de la base de datos, los ″spams″ enviados son ilegales.
- Quien remitió los ″spams″ ilegales, también es responsable de la violación de la privacidad de los datos personales.

Capítulo IV

HÁBEAS DATA

SUMARIO: 1. Introducción; 2. Concepto; 3. Naturaleza jurídica del hábeas data; 4. Los derechos tutelados por la acción de hábeas data; 5. El derecho procesal constitucional del hábeas data; 6. La acción de hábeas data en el texto constitucional; 7. Algunos aspectos procesales de la acción de protección de los datos personales (Ley 25.326); 7.1. Procedencia; 7.2.- Legitimación; 7.2.1. Legitimación Activa; 7.2.2. Legitimación Pasiva; 8. Objetivos del hábeas data; 9. Objeto de la acción; 10. La notificación previa; 11. Requisitos de la demanda de hábeas data; 12. Tipos y subtipos de hábeas data en el derecho constitucional latinoamericano; 12.1. Hábeas data informativo: subtipos exhibitorio, finalista y autoral; 12.2. Hábeas data aditivo: subtipos actualizador e inclusorio; 12.3. Hábeas data rectificador o correctivo; 12.4. Hábeas data reservador; 12.5. Hábeas data exclutorio o cancelatorio; 13. Derecho comparado; 13.1. En el ámbito internacional; 13.2. En el derecho comparado europeo; 13.2.1. Constitución Portuguesa de 1976; 13.2.2. Constitución Española de 1978; 13.2.3. Francia; 13.2.4. Reino Unido; 13.3. Derecho comparado en las Américas; 13.3.1. Canadá; 13.3.2. Estados Unidos; 13.3.3. Guatemala; 13.3.4. Colombia; 13.3.5. Brasil; 13.3.6. Paraguay; 13.3.7. Perú; 13.3.8. Chile; 14. República Argentina; 14.1. Constituciones provinciales; 14.1.1. La Rioja; 14.1.2. Córdoba; 14.1.3. San Juan; 14.1.4. Río Negro; 14.1.5. Provincia de Buenos Aires; 14.1.6. Constitución de la Ciudad Autónoma de Buenos Aires.-

1.- Introducción

El hábeas data es la más joven y novedosa garantía constitucional para la defensa y protección de los derechos humanos -junto al amparo y al hábeas corpus- que nació con la difusión masiva de los datos personales y la tecnología informática.

Es una herramienta que permite acceder, rectificar, actualizar, bloquear o suprimir determinados datos que podrían llegar a afectar a la persona. El constante desarrollo de la informática ha creado la necesidad de una adecuada protección legal del derecho a la privacidad. Con dicho objetivo, la reforma de la Constitución Nacional de 1994 incluyó expresamente en su texto este novedoso instituto.

Desde la aparición en escena del art. 43, párrafo 3° de la Constitución Nacional, y ante la ausencia de norma reglamentaria, fértil fue el debate en torno a si el plexo constitucional resultaba o no operativo, pronunciándose el criterio mayoritario por la primera solución. Recién con la sanción de la ley 25.326 (Ley de protección de los datos personales)[160] el hábeas data quedó reglamentado.

Según Sagüés,[161] el origen de esta acción se explica en virtud del desarrollo del llamado poder informático. Para el prestigioso autor, el hábeas data trata de recomponer un cierto desequilibrio a la hora de la protección en este ámbito: pues -dice- quienes hacen informática tienen generalmente protección constitucional de su actividad en las reglas que tutelan la libertad de comerciar, de trabajar, inclusive en las que protegen la propiedad; en cambio, la situación no es la misma para los registrados en los archivos o bancos de datos, ya que éstos pueden contener información equivocada, antigua, falsa, o con potenciales fines discriminatorios, o lesiva del derecho a la intimidad de las personas.

Por eso, la acción pretende dar una respuesta transaccional a los derechos de unos y de otros. Es una especie y variante del amparo, de reciente origen, que tiene por fin proteger determinados derechos constitucionales ante los excesos del poder informático.

El propósito de este capítulo es analizar la garantía del hábeas data en su relación con el derecho a la intimidad, así como la evolución de este concepto frente a la revolución informática y telemática.

2.- Concepto

El hábeas data es, conforme lo sostiene cierta doctrina, es una garantía constitucional, un medio de protección y aseguramiento del derecho de autodeterminación informativa.[162]

Para otros autores, consiste en "un novísimo desprendimiento del trono del amparo genérico, una especificación del mismo en razón de la materia, motivo por el cual también se lo ha denominado amparo informativo o informático".[163]

Dentro de esta línea se ha indicado que el hábeas data protege un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física, y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo.[164]

Esta acción puede ser ejercida, en tanto garantía de un derecho individual personalísimo, por el titular del derecho a interponer la acción, en defensa de aspectos de su personalidad vinculados con su intimidad que no pueden encontrarse a disposición del público ni ser utilizados sin derecho.[165]

En pocas palabras, se trata de una acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

Para Sagüés es una garantía constitucional, especie y variante del amparo, de reciente origen, que tiene por fin proteger determinados derechos constitucionales ante los excesos del poder informático.[166]

3.- Naturaleza jurídica del hábeas data

En torno a este tema no hay consenso en la doctrina. Bergel lo ha caracterizado como un derecho humano de tercera generación.[167] Para Guastavino, se trata en última instancia de una garantía constitucional tendiente a proteger el derecho a la identidad personal.[168]

En igual sentido, Rivera señala que uno de los aspectos protegidos por el hábeas data es el derecho a la identidad personal.[169] Ekmekdjian lo califica como una garantía al derecho a la intimidad,[170] y Sagüés lo define como una subespecie de amparo.[171]

Por último, Badeni sostiene que su propósito es evitar que mediante el uso de la informática se pueda lesionar el honor o la intimidad de las personas, particularmente lo segundo.[172]

En cuanto a la denominación que se le ha dado existen variantes: hábeas data, protección de datos -data protection-, y también "protección de la informática y libertades".

El término "hábeas data" es quizás el más representativo, pues en una analogía con el tradicional hábeas corpus, significaría "tráigase la información". Es justamente esta facultad de "acceder" o "conocer" los datos que se tienen sobre el requirente lo que caracteriza al instituto que analizamos.

Vale decir que a la figura bajo estudio en algunos casos se la caracteriza como una "garantía instrumental polifuncional", capaz de tutelar una multitud de derechos (a la intimidad, a la privacidad, a la autodeterminación informativa, a la verdad, a la identidad, al honor, a la imagen, a la voz, a la información) y como consecuencia a una pluralidad de bienes.[173]

4.- Los derechos tutelados por la acción de hábeas data

Aunque la doctrina discrepa respecto a cual es exactamente el bien jurídico tutelado, no cabe duda que el derecho a la protección de los datos personales es ejercido a través de la garantía del hábeas data.

Esta garantía protege derechos intrínsecos de la persona humana (intimidad, privacidad, identidad, honor, dignidad, verdad), datos éstos de carácter personal que se encuentran almacenados en los bancos de datos y que deben ser protegidos.

Travieso sostiene que la protección de datos personales constituye un elemento indispensable para restaurar la comunicación en una sociedad democrática que se ha ampliado en cantidad y calidad de derechos.

La acción y participación de la persona en los datos tiene relación con el ejercicio de los nuevos derechos en una democracia actualizada por la tecnología.[174]

Rivas hace hincapié en la finalidad tuitiva de la privacidad que tiene el instituto, expresando que el "querer" del hábeas data es el destinado a obtener protección jurisdiccional con respecto a la conducta activa o potencial de los poseedores públicos de datos sobre una persona en tanto dicha conducta puede causarle perjuicio actual o eventual o los datos hagan a una esfera de privacidad insusceptible de ser "capturada" por ajenos.[175]

Desde una perspectiva coincidente con la de Rivas, aunque extendiendo la tutela del instituto a otros derechos, se ha sostenido que el mismo no sólo protege la privacidad, sino también la intimidad, el derecho a la información, el derecho al honor, el de la propia imagen o perfil personal, e incluso el denominado derecho a la dignidad humana.[176]

Palazzi, por su parte, sostiene que el hábeas data protege un complejo de derechos personalísimos, que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad.[177]

Bidart Campos, expresa que, en verdad, la doctrina y el derecho comparado en materia de hábeas data arrancan del derecho personal a conocer los propios datos obrantes en registros o bancos de datos y, de ahí en más, y una vez conocidos, a modificarlos, rectificarlos, ampliarlos, proteger los datos sensibles, suprimirlos, actualizarlos, impedir divulgación, etc.

No es fácil resumir en un vocablo único el concepto del bien jurídico y de los derechos a los que el hábeas data cubre en estos supuestos. No obstante, descubrimos coincidencias en algo fundamental: es la autodeterminación informativa, o la libertad informática, o la privacidad de los datos, lo que se quiere controlar y defender.

En torno de ese objetivo el hábeas data busca, en determinados casos y circunstancias, que ciertos datos queden reservados y que no se hagan públicos.[178]

Debe quedar en claro que no se ha pretendido bajo este título inserto en el presente capítulo agotar el importante número de opiniones vertidas en torno a los derechos amparados por esta garantía.

Constituyen sólo algunos de los tantos existentes criterios con que ha sido abordada la cuestión de los derechos y bienes jurídicos cuya protección se persigue a través de la acción de hábeas data.

El objetivo de la garantía, como ya hemos remarcado, finca en la protección de cualquier tipo de dato personal, íntimo o no íntimo, público o privado, y sea que esa información tenga o no repercusión en los derechos al honor y a la intimidad de las personas, por cuanto el espectro tuitivo se debe considerar ampliado a la imagen y dignidad personales, y también encuadrarse en el marco del alcance del denominado derecho a la "autodeterminación informativa".

Basta en tal sentido que los datos de carácter personal objeto de registración y tratamiento, puedan incidir, por la utilización, comunicación o difusión que de ellos se haga o pueda llegar a hacerse, en el ejercicio de cualquier libertad o derecho constitucionalmente reconocido.[179]

5.- El derecho procesal constitucional del hábeas data

El actual art. 43 de la Constitución Nacional sienta una norma procesal, dando tres garantías para el efectivo goce y ejercicio de los derechos fundamentales: el amparo, el hábeas corpus y el hábeas data.

Esto abre un abanico de defensas ante las circunstancias actuales y las futuras proyecciones de la informática. En algunos casos se dijo por nuestros tribunales: que el hábeas data es procedente, si de los registros surgen inexactitudes o discriminación, y que los interesados tienen libre acceso a la información comercial y crediticia, suprimiéndose la información a los diez años.

El olvido suele ser un defecto y la memoria una cualidad, pero esa doctrina limitante de la tutela a casos de falsedad y discriminación, desatiende los graves efectos de la informática, uno de los cuales es precisamente memorizar lo que no se debe, haya o no plazo para suprimir los datos.

Pues, si el crédito fue saldado, aunque no fuera falsa la información por su rastreo histórico, el olvido aparece como una cualidad y no un defecto, que debe ser considerado para permitir la redención moral y crediticia del ser humano.

6.- La acción de hábeas data en el texto constitucional

La reforma de 1994 incorporó al texto constitucional un remedio extraordinario y urgente, a fin de que las personas pudieran obtener el conocimiento de los datos a ellas referidos y de su finalidad, que consten en registros o bancos de datos públicos o privados y en su caso exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.

Sin nominarla expresamente, ya que la ley de necesidad de reforma nada había expresado sobre este capítulo,[180] esta directiva fue trazada por el constituyente como una especie dentro del género del amparo, reservándole al hábeas data el tercer párrafo del art. 43 de la Constitución Nacional.[181]

Este artículo integra el Cápítulo II "Nuevos Derechos y Garantías", pero es de destacar que en el mismo se omite mencionar y transcribir el nombre de la acción que se garantiza. Simplemente dice: *"...esta acción..."*.

7.- Algunos aspectos procesales de la acción de protección de los datos personales (Ley 25.326)

7.1.- Procedencia

El hábeas data constituye una acción flexible, elástica, calificación que la doctrina no tiene temor alguno en resaltar como la verdadera virtud de este instituto.[182]

Con el propósito de resultar garante del objeto perseguido y asegurar el exacto cumplimiento del deber de informar, la ley 25.326 contempla la vía jurisdiccional por medio de lo que titula como "acción de protección de los datos personales", la que procederá en los siguientes supuestos:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.[183]

7.2.- Legitimación

Luego de identificar los supuestos de procedencia, los arts. 34 y 35 se ocupan de la legitimación tanto activa como pasiva.

7.2.1.- Legitimación Activa

El artículo 34[184] señala que la acción puede ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, por sí o por intermedio de apoderado.

Quiroga Lavié sostiene que el hábeas data busca solamente que el particular damnificado tome conocimiento de los datos a él referidos y su finalidad. No podrá en consecuencia tomar conocimiento de datos de terceros, ni de otras circunstancias registradas, aunque tuvieran directa vinculación con el registro de datos personales materia de la acción.[185]

Sagüés añade que no se trata de una acción popular y que sólo puede articularla el afectado.[186] Por último, Gozaíni subraya que la necesidad de acreditar el derecho subjetivo vulnerado es imprescindible pues se tutelan intereses propios que hacen a la naturaleza e imagen de una persona.[187]

Pero no debe descartarse tampoco la posibilidad de ejercer una suerte de "hábeas data colectivo" en los casos de discriminación, lo que se ve posibilitado por una interpretación conjunta del párrafo 2º[188] art. 43.[189]

Al no hacer distinción, se entiende que se posibilita su ejercicio tanto a personas individuales como colectivas, pues donde la ley no distingue el intérprete tampoco debe hacerlo. Claro está que tratándose de una persona jurídica no será el derecho a la intimidad el que esté afectado, pues este último no se predica de aquéllas.

Se ha dicho que frente a un ente ideal el hábeas data protege un derecho a la verdad sobre los datos sociales que se posean en un determinado registro y que hagan a la reputación, fama y buen nombre del afectado.[190] Puccinelli señala la posibilidad de que sea el propio Estado el accionante, cuando éste actúa en el campo del derecho privado.[191]

7.2.2.- Legitimación Pasiva

El artículo 35[192] prevé que el reclamo podrá ser dirigido en contra de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. Al hablar de "registros" o "bancos de datos" se debe entender que se hace alusión tanto a los ficheros manuales como a los informatizados.

En relación a los registros públicos, se sigue la tendencia del derecho comparado y es ésta una de las finalidades primordiales del hábeas data. El contemplar los registros públicos tiene su razón de ser en que cada vez es mayor el uso de registros informáticos que se nota en este sector.

En este momento cabría plantearse el interrogante respecto a si es necesario agotar la vía administrativa en el caso que la acción se dirija contra un banco de datos público.

Aunque lo lógico parecería requerir a la Administración previamente los datos, de acuerdo con la lectura del texto constitucional, el amparo puede interponerse siempre que no exista otro medio judicial más idóneo (art. 43 Constitución Nacional), por lo que parece haberse eliminado la necesidad de agotar la vía administrativa.

8.- Objetivos del hábeas data

Clásicamente se le asignan cinco objetivos al hábeas data:

a) De *acceso* a la información;
b) *Rectificación* de datos inexactos;
c) De *actualización* de la información;
d) De exigir la *confidencialidad* de determinados actos y
e) De exigir la *eliminación* de la información sensible o falsa.

Si bien nuestra Constitución garantiza todos estos derechos, no ha seguido el modelo de las reglamentaciones extranjeras que ofrecen conjuntamente las cinco opciones. Con una redacción diferente señala que toda persona tiene derecho a conocer los datos a ella referidos y su finalidad y en caso de falsedad o discriminación, -lo que deberá ser demostrado por el requirente-, se podrá acceder a los demás derechos: supresión, rectificación, confidencialidad o actualización.

Vale decir que sólo si existe una falsedad o se prueba que hay una discriminación se podrá ejercer una acción sobre los datos que sea mayor al simple conocimiento de los mismos y su finalidad. Por otra parte debe distinguirse la falsedad de la discriminación en cuanto a sus efectos. En el primero sólo tendrá sentido pedir supresión, rectificación o actualización, pero no la confidencialidad. En el segundo caso, el paso más lógico parece pedir la supresión del acto lesivo.

El art. 43 permite en una primera etapa el ejercicio de la acción de la persona afectada tendiente a tomar conocimiento de los datos a ella referidos y de su finalidad. Es decir que el accionante busca conocer no sólo qué datos se tiene sobre su persona en el registro sino también con qué objetivo ellos están en el registro.

La toma de conocimiento implica el ejercicio del derecho de acceso a la información. Este derecho de acceso tiene por finalidad permitir al individuo el control sobre la información que le concierne.

Una vez que se ha tomado conocimiento del dato y de su finalidad, se deberá probar que existe una falsedad o una discriminación para poder acceder a los otros derechos. En cuanto a la falsedad, será necesario demostrar que el dato no está de acuerdo con la realidad.

La supresión busca eliminar el dato erróneo -falso o discriminatorio-, que afecta la verdad o la igualdad. Vale decir que el borrado del dato enfrenta el derecho de propiedad del operador del banco de datos con la privacidad del individuo registrado.

Creemos que la solución adecuada -que contemple ambos valores-, consistirá en eliminar el dato si se logra probar que el mismo es falso o que causa algún perjuicio. En este sentido la tipología que adopta nuestro hábeas data, al permitir suprimir el dato sólo si hay discriminación o falsedad parece haber querido conciliar ambos valores.

Se podría admitir la supresión cuando el dato ha entrado erróneamente al registro, o cuando los datos personales ya no sean necesarios para los fines que contemplaron su almacenamiento.[193] También cuando el dato tenía otra finalidad y llegó al registro al que se accede por una vía ilegítima o sin consentimiento del registrado.

El caso de la rectificación busca precisión o fidelidad en los datos.[194] Una variante de esta rectificación es la posibilidad de actualización que también contempla el art. 43. Tales derechos pueden ejercerse contra registros públicos -por ejemplo, para que figure una absolución o un sobreseimiento-, también privados -vgr. para el caso de figurar como deudor o quebrado cuando no se tiene tal estado-.

En cuanto al pedido de confidencialidad, el mismo tiende a proteger la intimidad del individuo aislando datos sensibles. Tal sería el caso de preservar las enfermedades que figuren en la historia clínica o de impedir la identificación de un portador de HIV.

Por último, el texto del art. 43 finaliza con una frase que puede llevar a confusión a sus intérpretes acerca de la finalidad de este instituto, al mentar que *"no podrá afectarse el secreto de las fuentes de información periodísticas".* Badeni opina que la parte final de dicho artículo consagra un secreto periodístico que tiene carácter absoluto.[195]

Coincidimos plenamente con Gaibrois, en cuanto que esta última oración no guarda íntima relación con el tema en cuestión, ya que éste lo excede largamente y fue incluida a pedido de los órganos periodísticos que se pronunciaron en contra del derecho de réplica.[196]

9.- Objeto de la acción

El objeto de esta acción es tomar conocimiento de los datos y de su finalidad. Se podrá en consecuencia exigir la supresión, si los datos fueran falsos o discriminatorios. Su rectificación, si fueran equivocados o inexactos. Su confidencialidad, si fueran datos sensibles. O su actualización, si los datos no condicen con el estado o realidad actual del sujeto.

10.- La notificación previa

El art. 14 de la ley 25.326, en su segundo inciso[197], prevé, dentro del Capítulo III "Derechos de los titulares de datos", el "Derecho de acceso", explicando que el responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Una vez vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data.

Como se puede advertir, la norma reglamentaria crea un requisito de admisibilidad de la demanda de hábeas data, exigiendo la intimación previa al responsable o usuario de los bancos de datos públicos o privados.

En este sentido, Francisco Junyent Bas y Fernando Flores, entienden que deviene inconstitucional que la ley 25.326 exija como requisito de admisibilidad de la acción el reclamo previo ante el responsable del registro público o privado, pues al tratarse el hábeas data de una especie de amparo, no puede contrariar lo dispuesto por el párr. 1° del art. 43 de la Constitución Nacional, en especial el postulado de *"expedita y rápida".*[198]

La notificación previa -entienden- desvirtúa plenamente la naturaleza del hábeas data, haciendo añicos las orientaciones dadas por el constituyente, quien previó una vía jurisdiccional sumaria, precisamente atendiendo al bien jurídicamente tutelado.[199]

11.- Requisitos de la demanda de hábeas data

El título del art. 38[200] de la ley indica que la norma reglamenta los requisitos de la demanda para la acción de protección de datos de carácter personal.

Comienza el inc. 1º del art. 38[201] disponiendo que la demanda deberá ser interpuesta por escrito. Requiere la norma la individualización con la mayor precisión posible del nombre y domicilio del archivo, registro o bancos de datos y, en su caso, el nombre del responsable o usuario del mismo.

Desde ya se advierte que si bien es posible que los bancos o registros de datos personales reciban alguna denominación con fines comerciales o administrativos, y que pueda asignárseles alguna localización física a los locales o dependencias en los que desarrollan actividades y se encuentra su administración, lo trascendente a los fines procesales es la determinación del responsable o usuario accionados y su domicilio.

Bien puede ocurrir que los archivos o las terminales principales de los sistemas se encuentren ubicados en un domicilio, y que los responsables o usuarios de los bancos o bases de datos tengan registrado como domicilio del fichero -de acuerdo con el art. 21[202]- otro emplazamiento.

En el caso de los bancos públicos de datos el inc. 1º del art. 38[203] preceptúa que deberá procurarse establecer el organismo estatal del cual dependen,

requerimiento enderezado a dar participación a los auténticos responsables de esos ficheros.

En lo que hace a la fundamentación de la demanda, el inc. 2º[204] del artículo bajo comentario, establece dos supuestos diferenciados, el primero específico del denominado "hábeas data informativo", y el segundo relativo a la acción promovida con el objeto de "incidir" sobre los datos registrados.

Respecto del primero requiere que el accionante alegue las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona.

Es decir que se exige a quien promueve la acción, fundamente los motivos en los cuales basa su pretensión de "acceder" al archivo o registro del responsable o usuario accionado. Este recaudo aparece como innecesario si se tiene en cuenta que para la "admisibilidad" de la acción debe justificarse el cumplimiento de los recaudos que hacen al ejercicio de los derechos que reconoce la ley.

Si debe acreditarse haberse concretado la pretensión del ejercicio al derecho de "acceso" en los términos del art. 14[205], y si de acuerdo con dicha norma para que quede "expedita" la acción tiene que encontrarse vencido el plazo para la evacuación del informe, o considerarse el informe producido insuficiente, va de suyo que tal acreditación implicará necesariamente la justificación de las razones para acceder judicialmente a los datos personales presumiblemente registrados en el archivo.

La fundamentación en estos casos se reducirá, o bien a hacer notar el vencimiento del plazo legal para informar, o bien a exponer los motivos por los que se ha considerado insuficiente el informe proporcionado.

En lo que hace al segundo de los supuestos, se exige que el accionante alegue los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta, que dependerá de la génesis de la acción promovida. Si ella resulta producto del ejercicio extrajudicial del derecho de

acceso, tendrá razonabilidad efectuar tal alegación, ya que deberá motivarse la "incidencia" sobre los datos informados por el archivo.

Si, por el contrario, la pretensión esgrimida es consecuencia del requerimiento de supresión, rectificación, etc., esgrimido en ejercicio de los derechos otorgados por el art. 16[206], la justificación del ejercicio previo de estos derechos y de la negativa a acogerse lo peticionado por parte del responsable o usuario requeridos, hará devenir en superabundante la exigencia de brindar mayores motivaciones en ocasión de promoverse la demanda de hábeas data.

No obstante lo expresado, será menester en este caso brindar una sucinta explicación de la improcedencia o irrazonabilidad de la negativa formulada por el responsable o usuario, a aceptar la pretensión concretada previamente en ejercicio del derecho concedido por el referido art. 16 de la ley.

El inciso bajo análisis sólo ha previsto como presupuestos invocables de la demanda, la inexactitud, falsedad o carácter discriminatorio de la información, obviando otras posibles motivaciones fundantes de la promoción de la acción. La enunciación formulada no debe interpretarse como una cortapisa legal, sino simplemente como una enumeración no restrictiva.

En todos los supuestos de violación de las obligaciones reguladas en la Ley de Protección de los Datos Personales, relativos a la calidad de los datos y a su modalidad de tratamiento en todas sus etapas, como igualmente a los concernientes a los bancos de datos, a sus responsables y usuarios, y a las demás personas involucradas en dichas operaciones, será procedente la promoción de la acción de protección prevista en la norma, resultando tales violaciones supuestos invocables fundantes de la misma.

A modo de simple ejemplificación será posible promover dicha acción para requerir:

a) La supresión de datos registrados utilizados en violación a las finalidades que motivaron su recolección;

b) El sometimiento a confidencialidad de datos personales que sean merecedores de reserva;

c) La actualización de datos;

d) La supresión de datos caducos, etc.

Estas finalidades, entre muchas otras, superan el estrecho elenco de la "discriminación, falsedad o inexactitud" previsto en el inc. 2º del art. 38 bajo comentario. El supuesto de la invocación del carácter "discriminatorio" de la información, extensamente analizado al comentarse otras disposiciones de la ley, debe ser objeto de una ponderación adecuada, toda vez que en numerosas ocasiones habrá de resultar dificultoso el establecimiento de tal calidad en los datos de carácter personal.

En realidad cualquier dato puede llegar a considerarse discriminatorio, ya que en definitiva ello dependerá en gran medida del modo o la forma en que es interpretada y utilizada la información. Frente a esta situación podría verse entorpecida cualquier tentativa de acumulación o tratamiento de datos personales.

Para establecer algún parámetro que permita distinguir cuál de este tipo de información debe ser considerada discriminatoria y cuál no, será menester contrapesar la incidencia del archivo de los datos con las necesidades sociales que justifican su tratamiento.

Se ha interpretado que las alegaciones exigidas por la norma en ocasión de promoverse la demanda constituirían una suerte de "carga probatoria" para el accionante[207], lo que aparece como excesivo en razón de no implicar ese requerimiento legal la imposición de acreditación alguna.

Su exigencia obedece a la debida fundamentación de la acción, pero no se encuentra relacionada con la actividad probatoria, la que se corresponderá con otras prescripciones aplicables al proceso de la acción de hábeas data.

El inc. 2º del art. 38[208] concluye prescribiendo como requisito de la demanda, el de justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. El precepto alude a la acreditación del ejercicio previo, de los derechos otorgados a los titulares de los datos por los arts. 14[209] y 16[210] de la ley.

En tal sentido los arts. 14, inc. 2º y 16, inc. 3º de la ley preceptúan, el primero que vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley (en relación a la pretensión de "acceso" concretada), y el segundo que ante la pretensión de rectificación, actualización, etc. formulada, vencido el plazo otorgado por la ley para acogerla, el incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

La conjugación de la acreditación exigida por el inc. 2º del art. 38 con lo dispuesto por las normas transcriptas precedentemente, implica la consagración de la "reclamación extrajudicial previa" como recaudo de admisibilidad de la acción de protección de datos personales. La ley se ha inclinado por exigir esta reclamación previa, requerida por unos[211] y rechazada por otros[212] antes de la entrada en vigencia de la normativa.

Esta acreditación requerida por el art. 38 tendrá aplicación en todo el ámbito de vigencia de la ley 25.326, subsistiendo las incógnitas interpretativas en todas aquellas jurisdicciones donde las disposiciones del capítulo VII de la ley en cuestión no tienen vigencia.

En esas jurisdicciones, no obstante reconocerse la existencia de precedentes jurisprudenciales en ambos sentidos, y de que con el arribo de la ley reguladora de la tutela de los datos personales sus prescripciones empero no tener vigencia, pueden ejercer un efecto de "persuasión moral", se considera más ajustado a derecho obviar el requerimiento del recaudo.

12.- Tipos y subtipos de hábeas data en el derecho constitucional latinoamericano

Como el hábeas data ha sido concebido principalmente para tutelar a los derechos de los particulares frente a quienes colectan, tratan o distribuyen datos -ya sean otros particulares o el Estado-, se encuentra más perfeccionado para estos fines que para su otra versión, que pretende brindar una herramienta efectiva tanto a

quienes colectan información ante la negativa injustificada de acceso a las fuentes de información pública, como a la sociedad, que también cuenta con el derecho a informarse a través de quienes luego de recabada la información, la proyectarán hacia ella.

En el caso de Argentina, el tema relativo a los datos personales y al acceso a la información pública ha tenido regulaciones diversas. Mientras algunas de las provincias consideraron en sus constituciones sólo un aspecto de la protección de aquellos datos, ocupándose de los antecedentes policiales y penales (La Rioja, Salta y San Juan), o de establecer el derecho de acceso a las fuentes de información (Catamarca y Formosa, además de Río Negro y San Luis, que por otra parte también regularon el hábeas data), otras fueron más allá, consagrando al hábeas data como acción específica de garantía (Ciudad Autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, La Rioja, Jujuy, Río Negro, San Luis, San Juan y Tierra del Fuego), aunque con diseños bien diversos. Además de la regulación constitucional, o en vez de ella, algunas provincias asumieron el tema en la legislación subconstitucional (v.gr., Tucumán, Jujuy).[213]

Sagüés[214] ha distinguido varios tipos y subtipos de hábeas data en el derecho constitucional contemporáneo, en una clasificación que consideramos ampliamente clarificadora.

12.1.- Hábeas data informativo: subtipos exhibitorio, finalista y autoral

Explica Sagüés, que el hábeas data informativo es aquel que procura solamente recabar información, y se subdivide en los subtipos:

- *exhibitorio:* (el conocer qué se registró);
- *finalista:* (determinar para qué y para quién se realizó el registro); y
- *autoral:* (cuyo propósito es inquirir acerca de quién obtuvo los datos que obran en el registro).

A estos subtipos, cabe agregar dos, emergentes por lo general de la regulación subconstitucional o de otras normas constitucionales:

- Aquel que tiene por objeto indagar sobre la existencia y localización de bancos y bases de datos (varios países -v.gr., España, a través de su LORTAD o Ley Orgánica Relativa al Tratamiento Automatizado de Datos-, con el objeto de garantizar el ejercicio de los derechos de aquellos que se encuentren potencialmente afectados, establecen la obligatoriedad de inscribir a las bases y bancos de datos en un registro especial), ya que para poder ejercer los derechos reconocidos por las normas protectoras de datos personales resulta

obvio que es necesario previamente localizar las fuentes potencialmente generadoras de información lesiva;[215] y

- Aquel que pueden utilizar aquellos que pretenden acceder a la información pública, cuando no se les permite el acceso a ella sin la debida justificación (obligación legal de reserva, motivos de seguridad del Estado, etc). Contienen regulaciones relativas al derecho típico de este último subtipo las constituciones de España y del Perú, y en el plano interno argentino, las constituciones del Chaco, Formosa, Río Negro, San Luis y San Juan, que mencionan el derecho de libre acceso a las fuentes de información. Establecen excepciones expresas al principio, admitiendo restricciones de acceso a la información para los casos de los asuntos vitales para la seguridad del Estado.[216]

12.2.- Hábeas data aditivo: subtipos actualizador e inclusorio

Este tipo procura agregar más datos a los que figuran en el registro respectivo. En él confluyen dos versiones distintas: puede utilizarse tanto para actualizar datos vetustos, como para incluir en un registro a quien fue omitido.[217]

Regulan expresamente la versión actualizadora las constituciones de Argentina, Brasil, Colombia y Paraguay. También lo contienen la de Portugal y las cartas de la Ciudad Autónoma y de la Provincia de Buenos Aires, Córdoba, Chaco, Chubut, San Juan y Tierra del Fuego.

12.3.- Hábeas data rectificador o correctivo

Su misión es la de corregir o sanear informaciones falsas, y también podría abarcar a las inexactas o imprecisas, respecto de las cuales es factible solicitar determinadas precisiones terminológicas, especialmente cuando los datos son registrados de manera ambigua o pueden dar lugar a más de una interpretación.

Este tipo se encuentra regulado en las siguientes constituciones: Argentina, Brasil, Colombia, Guatemala y Paraguay. Lo prevén también expresamente la Constitución de Portugal y en el orden interno argentino las de la Ciudad Autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, Jujuy, San Juan y Tierra del Fuego.

12.4.- Hábeas data reservador

Se trata de un tipo cuyo fin es asegurar que un dato que se encuentra legítimamente registrado, sea proporcionado sólo a quienes se encuentran legalmente autorizados para ello y en las circunstancias en que ello corresponde.

En la Argentina, al tiempo de reformarse la Constitución nacional en 1994, este tipo de hábeas data no se encontraba previsto en los dictámenes de la mayoría ni de la minoría en la Convención Constituyente, y se debió a una propuesta del convencional Cullen, quien mencionó la necesidad de incorporar este derecho.[218]

Pese a que ello fue aceptado en el seno de la Convención y parece de toda lógica que determinados datos sean registrados pero no trasciendan a terceros sino sólo excepcionalmente (v.gr., aquellos datos "sensibles"[219] que sea necesario tener registrados, como los relativos al estado de salud de la persona registrada), en disconformidad con la previsión, Bergel entiende que la confidencialidad no es meta propia de esta garantía.[220]

Esta posición sólo se entiende si se parte de una interpretación literalista del art. 43 de la Constitución Nacional, y se limita al hábeas data sólo cuando exista falsedad o discriminación, y se visualiza que en tales casos no corresponde sino la cancelación del dato y no su confidencialización. De todas formas, nos parece que puede ser suficiente con la reserva del dato para eliminar la potencial discriminación.

Palazzi, advirtiendo las deficiencias de la formulación constitucional, también indica que en el caso de falsedad tendrá sentido pedir supresión, rectificación o actualización, pero no la confidencialidad de los datos, y que cuando éstos fueron recabados con el propósito de discriminar, el paso más lógico parece el de pedir la supresión del dato.[221]

Este tipo se encuentra regulado en las constituciones de Argentina y Perú. También lo prevén expresamente las constituciones de Portugal y -ya en el ámbito interno argentino-, las de la Ciudad Autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, Jujuy y Tierra del Fuego.

12.5.- Hábeas data exclutorio o cancelatorio

Este tipo tiene por misión eliminar la información del registro en el cual se encuentre almacenada, cuando por algún motivo no debe mantenerse registrada.

Sagüés, entiende que la eliminación procede en los casos en que se trate de datos denominados "sensibles" y menciona que no existe una regla fija acerca de cuándo es procedente un hábeas data para "reservar", y cuándo el contenido peligroso de esa información es tan grande que corresponde borrarla, y que el criterio delimitante varía según cada sociedad y su momento histórico, pues datos que otrora

no eran vistos como nocivos, asumen hoy en ciertas comunidades rasgos tan altamente negativos que parece indispensable eliminarlos.

Este tipo se encuentra regulado expresamente en las constituciones de Argentina y Paraguay. También lo prevén expresamente las constituciones de Portugal -aunque limitado al caso de la informática-, Ciudad Autónoma y provincia de Buenos Aires, Chaco y Chubut.

Las diferencias resultantes en las regulaciones antes vistas muchas veces provocan confusiones conceptuales[222] y consecuentemente llevan a amputaciones innecesarias del hábeas data, el que debe ser regulado -constitucionalmente hablando- de una manera simple y abierta, de forma tal que permita la adecuación a las más variadas posibilidades y a los cambios por venir.

Es que, como indica Vanossi[223], el secreto del hábeas data está, precisamente, en su sencillez. Si al hábeas data se lo convierte en un mecanismo complejo demasiado sofisticado y articulado, no va a ser captado y entendido por los propios interesados, es decir, por los ciudadanos o por los habitantes, que van a encontrar dificultades en el acceso al mismo para poderlo esgrimir y utilizar como herramienta protectora.

Tiene que ser algo muy simple, muy sencillo, muy informal (quizás ésta sea la palabra que más cuadra a la descripción de la situación), para que cualquiera que se pueda sentir afectado por informaciones monopólicas que lo afectan o lo perjudican en su status, pueda entonces remover ese obstáculo tendiendo fundamentalmente a dos cosas: el derecho a la rectificación, a la anulación de aquellos asientos que puedan ser lesivos o perjudiciales.[224]

13.- Derecho comparado

La problemática relativa al derecho a la protección de los datos personales ha sido abordada en diversos instrumentos internacionales tanto de la Organización de Naciones Unidas (ONU) y del Consejo de Europa, como de otras organizaciones internacionales; también, en la propia Unión Europea.[225]

Además, ha quedado plasmada como preocupación constitucional y legislativa en numerosos países de Europa y de América.

13.1.- En el ámbito internacional

En el plano del derecho comunitario europeo, emerge como instrumento de gran importancia la Directiva 95/46/CE del 25 de octubre de 1995 del Parlamento Europeo y el Consejo.[226]

Tal Directiva se refiere a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos, y a la misma debían quedar ajustadas (al 25 de octubre de 1998) las preceptivas internas de los Estados componentes de la Unión Europea, lo que provocó un intenso movimiento legislativo en tal sentido.

Ello, con el objeto de eliminar la disparidad que entre tales normativas legales surgía en relación con los niveles de protección de los datos, circunstancia que podría funcionar como óbice para su transmisión de información entre dichos Estados.[227]

Por su parte, en la Carta de Derechos Fundamentales de la Unión Europea, de 2000, se reconoce el derecho de protección de datos de carácter personal, los que se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. También expresa que toda persona tendrá derecho a acceder a los datos recogidos que la conciernan y a su rectificación.[228]

En el contexto de la Organización de los Estados Americanos (OEA), un buen paso adelante significaría la aprobación de una Convención Americana para la Autodeterminación Informativa. Actualmente, sólo existe en etapa embrionaria un borrador o anteproyecto de la misma, bajo el epígrafe de "Garantías judiciales", se prevé el derecho de toda persona a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que los ampare contra actos que violen sus derechos fundamentales reconocidos por la Convención, la Constitución de los Estados Partes o la ley.[229]

Para tal fin consagra el derecho de toda persona a controlar sus datos personales existentes en ficheros públicos o particulares, señalando que la garantía y el procedimiento judiciales para ejercer tal control es el hábeas data. Además, y si bien defiere al derecho interno de los Estados la regulación de la naturaleza constitucional o común de tal recurso, indica que en todo caso éste debe ser su medio de amparar en forma expedita, rápida y eficaz los derechos de la persona ante los excesos informáticos automatizados o manuales.

Básicamente el objeto de la protección del anteproyecto de Convención consiste en garantizar, en el territorio de cada Estado Parte, a cualquier persona física o jurídica sean cuales fueren su nacionalidad, residencia o domicilio, el respeto de sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa con relación a su vida privada y demás derechos de la personalidad,

además de la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

13.2.- En el derecho comparado europeo

En este punto haremos una recorrida por los principales instrumentos y cuerpos normativos de Europa y también de América, observando y puntualizando cuáles son, si existen, las diferencias entre los diversos esquemas legislativos.

13.2.1.- Constitución Portuguesa de 1976

Fue Portugal el primer país europeo que reconoció constitucionalmente (en 1976) la necesidad de proteger a las personas frente a los riesgos informáticos. No obstante ello, hubo de transcurrir un período de quince años para que aquellas disposiciones fueran desarrolladas legislativamente.

En efecto, en abril de 1991 se dictó la ley 10 de protección de datos personales frente a la informática; normativa que amplía los parámetros tuitivos de la Constitución; establece que el uso de la informática debe procurarse de forma transparente y con estricto respeto por la reserva de la vida privada y familiar y de los derechos, libertades y garantías fundamentales del ciudadano; prevé la creación de la autoridad de aplicación (Comisión Nacional de Protección de Datos Personales Informatizados); determina que ninguna decisión judicial, administrativa o disciplinaria puede tomarse sobre la exclusiva base del perfil de personalidad del titular del registro del banco de datos; y, en síntesis, reproduce los principios consagrados por el mencionado Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa[230].

La constitución de este país, consagra el derecho de los ciudadanos a tomar conocimiento de sus propios datos en registros informáticos pudiendo exigir su rectificación y actualización, consagra asimismo la protección a los datos sensibles.

13.2.2.- Constitución Española de 1978

Garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Establece que la ley limitará el uso de la informática para garantizar tales derechos.

El Estado Español en la actualidad posee la ley orgánica 15/99 de Protección de Datos de Carácter Personal, cuyo objeto es precisamente garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar.[231]

13.2.3.- Francia

Dictó la ley Nro. 78-753 del 17 de julio de 1978. Ésta consagra el derecho de toda persona a la información y el respeto a la privacidad estableciendo medidas de mejora de las relaciones entre la administración y la población como asimismo disposiciones de carácter administrativo, social y fiscal.

13.2.4.- Reino Unido

La ley de Protección de Datos del año 1988 ha sido objeto de modificaciones, luego de un proceso de consulta acontecido en el año 1999 y con ella se ha modificado también la ley de Acceso a la información (Freedom of information act. 2000).

En el ámbito comunitario europeo los Estados miembros del Consejo de Europa suscribieron en la Ciudad de Estrasburgo el 28 de enero de 1981 el Convenio para la Protección de Personas con respecto al tratamiento automatizado de datos de carácter personal".[232]

Este convenio tiene por objeto y fin regular el tratamiento automatizado de datos de carácter personal para proteger el respeto a derechos y libertades fundamentales de las personas físicas con independencia de su nacionalidad o residencia.

Asimismo se destaca la Directiva 95/46/CE del 24 de octubre de 1995 relativa a protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.[233]

Esta Directiva es de suma importancia, pues crea un Grupo de Trabajo cuya función es evaluar a los Estados y a través de Decisiones determinar si califican o no como Estados que garantizan un adecuado nivel de protección de los datos personales que se transfieren desde la Comunidad.

13.3.- Derecho comparado en las Américas

13.3.1.- Canadá

En el año 1982 sancionó la ley de acceso a la información consagrando el respeto a la privacidad y acceso a la información.

13.3.2.- Estados Unidos

En 1966 sancionó la ley de libertad de información FOIA - (The Federal Freedom of information Act). Diez años después fue dictada una enmienda a la ley con relación a los documentos electrónicos.[234]

Más tarde, con exactitud en 1974, se sancionó la Ley de Privacidad (Privacy Act), aunque el concepto de "privacy" ya había surgido en la jurisprudencia y doctrina norteamericana a fines del siglo XIX.

Esta norma otorga el derecho a todo ciudadano o residente a consultar información que sobre su persona el Estado posea (salvo estrictas excepciones) faculta a solicitar la corrección de prontuarios, a ser informado de cuándo y cómo es usada tal información por entidades públicas. La ley crea una acción civil ante la justicia para demandar por daños y perjuicios.

13.3.3.- Guatemala

La Constitución Política de la República de Guatemala del año 1985 consagra a toda persona el derecho a conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales y su finalidad con facultad de corregirlos rectificarlos y actualizarlos.[235]

13.3.4.- Colombia

La Constitución Colombiana de 1991 consagra el derecho a la intimidad personal y familiar, obligando al Estado a respetarlos y hacerlos respetar asimismo consagra el derecho de las personas a conocer, actualizar y rectificar las informaciones que se hallan recogido sobre ellas en los bancos de datos y en los archivos privados.[236]

13.3.5.- Brasil

Fue el primer Estado en nuestro continente en consagrar al hábeas data. Y lo llevó a cabo en la constitución promulgada en octubre de 1988.

En dicho cuerpo normativo señala que debe concederse el hábeas data para asegurar el conocimiento de informaciones relativas a la persona del peticionario que consten en registros o bancos de datos de entidades gubernamentales o de carácter privado, señala asimismo para la rectificación de datos, cuando no se prefiera hacerlo por proceso sigiloso, judicial o administrativo. Además, consagra la gratuidad de este procedimiento.[237]

13.3.6.- Paraguay

Su actual constitución sancionada y promulgada en junio de 1992 consagra el hábeas data a toda persona para acceder a la información y a los datos propios o sobre sus bienes, que obren en registros oficiales o privados de carácter público, para conocer el uso y finalidad de los mismos.

Resulta de gran importancia las disposiciones referidas a la competencia y responsabilidad de los magistrados. Señala que si el magistrado competente se negare injustificadamente, a entender en esta acción será enjuiciado y, en su caso, removido. Otorga asimismo al magistrado interviniente facultades sancionatorias para los agentes responsables.[238]

13.3.7.- Perú

Su Constitución Política de 1993 establece la acción del hábeas data como una garantía constitucional, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnere o amenace los derechos tutelados en la misma.

También refiere al derecho a solicitar información sin expresión de causa y a recibirla exceptuando las informaciones que afectan la intimidad personal, es decir, los denominados datos sensibles y las que se excluyan expresamente por disposiciones legales o por razones de seguridad.[239]

Perú además ha sancionado en el año 1994 la ley 26.301, esta norma establece la competencia para la tramitación de la acción de hábeas data y la "acción de cumplimiento" en forma conjunta, lo que dificulta un tratamiento sistemático de los mismos.[240]

13.3.8.- Chile

En el año 2000 dictó a la ley 19.628 de "Protección de Datos de Carácter Personal". Esta ley, tal como su nombre indica, tiene por objeto proteger datos

personales, pero únicamente de personas físicas. Pone especial énfasis y criterio amplio respecto al contenido de los datos sensibles, no así a su tratamiento.[241]

14.- República Argentina

14.1.- Constituciones provinciales

En la República Argentina, mucho antes de ser consagrado el derecho a la protección de los datos personales en el ámbito federal, lo fue en el derecho provincial.

14.1.1.- La Rioja

La Constitución de la Provincia de La Rioja del año 1986 consagra el derecho a la privacidad, expresando que la ley limitará el uso de la informática para preservar el honor, la intimidad personal y familiar de los habitantes y el pleno ejercicio de sus derechos. Respecto a datos que refieran a antecedentes penales, estos sólo serán proporcionados en los casos previstos por la ley.

14.1.2.- Córdoba

La Constitución de esta provincia data del año 1987, y refiere a la privacidad como derecho de toda persona a conocer lo que de ella conste en forma de registro, la finalidad a que se destine esa información y a exigir su rectificación y actualización.

Estos datos sólo se proporcionarán a terceros excepcionalmente cuando tengan un interés legítimo y no podrán ser usados con propósitos discriminatorios.

Establece asimismo que el uso de la informática será reglamentado por ley, de modo tal que no vulnere la intimidad personal y familiar.

14.1.3.- San Juan

Establece el derecho de todo ciudadano a conocer lo que de él conste en los registros y la finalidad a que tal información esté destinada, con facultad para solicitar

su rectificación y actualización. Establece también que la informática no podrá utilizarse para el tratamiento de datos sensibles (convicciones políticas, fe religiosa o vida privada) salvo que tal información sea destinada para fines estadísticos no identificables.

14.1.4.- Río Negro

En su Constitución de 1988 consagra el derecho a la privacidad estableciendo que la ley asegura la intimidad de las personas. Establece que el uso de la información almacenada, procesada o distribuida a través de medio físico o electrónico debe respetar el honor, la privacidad y el goce completo de los derechos.

Refiere de nuevo a que la ley reglamentará su utilización en consonancia con los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguarda de la seguridad, apertura de registros, limitación en el tiempo y control público.

Asegura el acceso de las personas afectadas a la información y su derecho a rectificarla actualizarla o cancelarla cuando no fuera razonable su mantenimiento.

Es importante aclarar que al decir "la ley" se refiere a la ley provincial 2384, que contempla el procedimiento, demanda, traslado y prueba por dos días, y cinco para dictar sentencia. Esta ley en efecto reconoce la protección de los derechos mencionados a través del hábeas data.

14.1.5.- Provincia de Buenos Aires

La Constitución sancionada en 1994 establece como garantía de los derechos constitucionales al hábeas data. Establece que toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o banco de datos de organismos públicos y privados destinados a proveer informes, así como la finalidad a que se destine esa información, y a requerir su rectificación, actualización o cancelación.

Casi similar de modo similar a la constitución federal establece que no podrá afectarse el secreto de las fuentes y el contenido de la información periodística.

También señala que los datos no podrán ser registrados con fines discriminatorios, y respecto a proporcionarlos a terceros, solo se hará cuando éstos tengan un interés legítimo. Establece asimismo que el uso de la información no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.

14.1.6.- Constitución de la Ciudad Autónoma de Buenos Aires

En la misma garantiza el derecho a la privacidad, intimidad y confidencialidad como parte inviolable de la dignidad humana. Expone que todas las personas tienen idéntica dignidad y son iguales ante la ley, reconociendo en consecuencia el derecho a ser diferente, no admitiendo discriminación alguna.[242]

Capítulo V

ANÁLISIS DE LA LEY 25.326

SUMARIO: 1. Introducción; 2. Antecedentes de la ley 25.326; 3. Objeto y alcance de la ley; 4. Bancos y bases de datos comprendidos; 5. Derechos reconocidos por la ley a los ciudadanos.-

1.- Introducción

A los fines de realizar un análisis de la ley 25.326 (Ley de Protección de los Datos Personales), hemos optado por destacar las políticas de tratamiento de datos personales adoptadas por nuestro país y, a partir de ello, elaborar una breve conclusión que contenga los aspectos puntuales de la citada norma, evitando así una interpretación exhaustiva de su articulado, lo cual excedería la meta propuesta en el presente trabajo y su desarrollo. Así mismo cabe resaltar que los puntos principales de la misma han sido desarrollados anteriormente en cada capítulo en particular.

2.- Antecedentes de la ley 25.326

En 1992 la Subsecretaría de Derechos Humanos -entonces dependiente del Ministerio del Interior- elaboró un anteproyecto de ley de hábeas data. Este anteproyecto ponía especial énfasis en el conocimiento de la información obrante en dependencias oficiales, incluso fuerzas armadas, policiales, penitenciarias y servicios de inteligencia.

Contemplaba para el caso de personas desaparecidas, la legitimidad del ejercicio de la acción a sus familiares. Con posterioridad el anteproyecto fue reformulado, pero en la realidad nunca dejó de ser tal.

Años después el Congreso Nacional sancionó la ley 24.745: "Hábeas Data y Protección de Datos Personales", cuyos cuarenta artículos fueron vetados por decreto 1616/96 del Poder Ejecutivo.

El 4 de octubre del año 2000 se sancionó al fin nuestra actual, la Ley de Protección de Datos Personales, bajo el N° 25.326. Y en el año 2001 se dicta el decreto 1558 que introduce las normas reglamentarias de la misma. La Ley 25.326 consta de 47 artículos divididos en VII Capítulos:

- Capítulo I - Disposiciones Generales (arts. 1 y 2).
- Capítulo II- Principios generales relativos a la protección de datos (arts. 3 al 12).
- Capítulo III - Derechos de los titulares de datos (arts. 13 al 19).
- Capítulo IV- Usuarios y responsables de archivos, registros y bancos de datos (arts. 21 al 28).

Estos cuatro primeros capítulos son aplicables en todo el territorio nacional.

- Capítulo V - Control (arts. 29 y 30). (34)
- Capítulo VI - Sanciones Penales (arts. 31 al 32).
- Capítulo VII - Acción de protección de los datos personales (arts. 33 al 47).

Estos tres últimos capítulos no son de orden público y es facultad de cada gobierno provincial suscribirlos o no. A este respecto, en la actualidad sólo la Provincia de Entre Ríos ha dado media sanción a la norma para tornarlos vinculantes.

Cabe mencionar que el Estado Argentino, en virtud a su ordenamiento jurídico en esta materia ha logrado ser incluido entre los Estados calificados como de máximo estándar sobre el nivel de protección de datos personales.

Ello fue así por Decisión de la Comisión de las Comunidades Europeas adoptada en sesión celebrada en Bruselas (Bélgica) el 30 de junio de 2003.

3.- Objeto y alcance de la ley

La ley 25.326 es una norma de orden público que regula la actividad de las bases de datos que registran información de carácter personal y garantiza al titular de los datos la posibilidad de controlar el uso de sus datos personales.

Este derecho a controlar la información personal, como derecho humano fundamental, debe interpretarse de manera amplia, concediendo al titular del dato el derecho a acceder a todo banco de datos para conocer la información que sobre su persona se encuentra registrada.[243]

En cuanto al objeto de la ley, el mismo consiste en la protección integral de los datos personales asentados en bancos de datos, sean éstos públicos o privados, destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.[244]

4.- Bancos y bases de datos comprendidos

Es importante dejar en claro que la 25.326 no abarca solamente a quienes comercializan bases de datos o quienes prestan servicios de información a

terceros. Por el contrario, la norma en cuestión adopta un criterio sumamente amplio, basado en la legislación sobre datos personales de España e Italia.

Así, por ejemplo, cuando una empresa informa a su contador el listado de sus clientes está cediendo datos personales a un tercero y, por consiguiente, se encuentra comprendida por la Ley de Protección de los Datos Personales.

Como ya hemos expresado, debe entenderse por banco de datos destinados a proveer informes a aquel banco de datos que permita obtener información sobre las personas, se transmitan o no a terceros.

Y como ya hemos señalado anteriormente, al tratarse de un derecho humano fundamental, la interpretación del cuerpo normativo debe ser amplia, a favor del titular del dato.

Por otro lado, no es necesario que el destino de brindar informes sea único y exclusivo. En ninguna parte de la norma se indica que para que la protección de la ley adquiera virtualidad debe tratarse de un destino único y exclusivo de brindar informes. Alcanza con que uno de los usos que se le da a la base de datos sea brindar información o describir algo sobre una persona determinada o determinable para que rija la protección de la ley.

Tampoco la norma exige que el destinatario del informe deba ser una tercera persona ajena al responsable o usuario de la base de datos, sino que también abarca los usos internos de la información personal.

En suma, se encuentra alcanzada por la ley 25.326 cualquier base de datos que, una vez accedida, permita obtener una descripción o informe de una persona determinada o determinable.

Para resumir, debemos resaltar que de la lectura y análisis de la normativa -exceptuando los aspectos procesales que ya han sido objeto de tratamiento en el presente trabajo- surge claramente que:

a) Se inscriben las bases de datos, no las personas, y la inscripción se renueva anualmente.

b) Deben inscribirse ante la Dirección Nacional de Protección de Datos todas las bases de datos que contengan datos de carácter personal que pertenezcan al sector público nacional y todas las demás, públicas o privadas (en este último caso, siempre que excedan del uso exclusivamente personal) que estén interconectadas en redes interjurisdiccionales, nacionales o internacionales.

c) Sólo se encuentran relevadas del deber de inscripción las bases que traten datos que no refieran a personas identificadas o identificables ("datos disociados") de conformidad con lo establecido en el art. 28[245] de la ley 25.326, aunque en realidad estarían también excluidas todas las que tratan datos disociados aunque no sean de las mencionadas en el mismo, pues el art. 2[246] de la ley no considera datos personales a aquellos que brinden información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

d) No se encuentran relevadas del deber de inscripción aquellas bases en las que pueden tratarse los datos sin consentimiento (con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia).

e) Deben inscribirse también quienes tratan datos por cuenta de terceros, aunque no tengan bases de datos propias.

f) La falta de inscripción acarrea, por un lado sanciones (leves o graves -cuestión que no es pasible de tratamiento en el presente trabajo-), y por el otro, la imposibilidad de colocar el isologotipo que la acredita como base de datos inscripta.

g) Las sanciones a las bases de datos que exceden del uso exclusivamente personal pero que no estén destinadas a dar información pueden controvertirse en virtud de no estar incluidas entre las sancionables ni en la ley 25.326 ni en el decreto 1558/2001.

5.- Derechos reconocidos por la ley a los ciudadanos

Los derechos que la Ley de Protección de Protección de los Datos Personales le reconoce a la ciudadanía en general son los que a continuación detallamos:

- *Oposición*

Derecho a negarse a facilitar un dato de carácter personal en el caso de que no sea obligatorio hacerlo.

- *Información*

Derecho a que en el momento en que se recolectan datos de carácter personal se le informe de modo expreso, preciso e inequívoco de las siguientes circunstancias:

- finalidad para la que serán tratados sus datos personales;
- quiénes pueden ser sus destinatarios;
- identidad y domicilio del responsable de la base de datos;
- carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga;
- consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
- y posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

- *Acceso*

Derecho a obtener información acerca de la siguientes circunstancias:

-Existencia de datos referidos a su persona en todo archivo, registro, banco o base de datos que contenga información personal;

-Fuentes y medios a través de los cuales se obtuvieron sus datos;

-Finalidad para la cual fueron recabados sus datos; y

-Destino previsto para sus datos.

- *Rectificación*

Derecho a exigir que los datos personales incluidos en un archivo, registro, banco o base de datos que sean inexactos o incompletos, sean rectificados o actualizados.

- *Supresión*

Derecho a exigir que se eliminen los datos personales que, por diversas circunstancias, no deban figurar en un archivo, registro, banco o base de datos, o que se supriman o sometan a confidencialidad los datos personales que sean inexactos o incompletos.

- *Tutela*

Derecho a iniciar acciones judiciales tendientes a tomar conocimiento de los datos personales almacenados en archivos, registros, bancos o bases de datos públicos o privados destinados a proporcionar informes y, cuando corresponda, a exigir su rectificación, supresión, confidencialidad o actualización, así como a reclamar los daños y perjuicios que pudiera haber sufrido como consecuencia de la inobservancia de la ley.

- *Impugnación*

Derecho a impugnar todo acto administrativo o decisión privada que implique una apreciación o valoración del comportamiento de un ciudadano fundado únicamente en el tratamiento de datos de carácter personal que permita obtener un determinado perfil de su personalidad.

- *Consulta*

Derecho a solicitar a la Dirección Nacional de Protección de Datos Personales información relativa a la existencia de archivos, registros, bases o bancos de datos personales y sus finalidades.

Conclusiones

En esta instancia cabe realizar una conclusión sobre los temas que se fueron analizando durante el transcurso del presente trabajo.

Podemos considerar a Internet como un nuevo espacio de socialización. Espacio que abarca mucho más que las fronteras de un país y que se ha extendido por todo el planeta.

La revolución tecnológica, con la informática como una de sus máximas expresiones, ha llegado para quedarse. Reiteradamente a los largo del presente trabajo hemos analizado sus impactos sobre la sociedad y, en especial, en el mundo del Derecho.

Recién en 1994, nuestro país comenzó a trazar un serio camino hacia el tratamiento de estos temas. Y en el 2000, se formalizó con el dictado de la ley 25.326 (Ley de Protección de los Datos Personales) a la cual le siguió su decreto reglamentario Nº 1558.

La tarea del Congreso constituyó un hito más en la escalada hacia el progreso de la Ciencia Jurídica y sembró una nueva semilla que seguramente germinará, en pro de producir como fruto las soluciones a los retos que plantea el avance tecnológico.

En referencia a la normativa local sobre la materia, como hemos observado, nuestra Ley de Protección de los Datos Personales no tiene grandes diferencias con las del resto de los demás Estados. Vemos que el problema en nuestro país -y no sólo en esta materia- es la aplicabilidad y el cumplimiento que tienen las normas.

No tiene sentido ni objeto contar con infinidades de leyes que reglamenten diversas cuestiones si no se les da cumplimiento a las mismas. Es un que permanece inserto en nuestra sociedad, caracterizada por evadir a menudo cada uno de los preceptos legislativos.

A nuestro parecer, y parafraseando aquella frase que expresa que: “el hombre es hijo del rigor”, ninguna ley sería exitosa si no hay temor al hecho de no cumplirla. Si bien pueden existir culturas más organizadas que otras, lo cierto es que nadie cumple por el sólo hecho de cumplir. Se cumple porque se teme al severo y preciso castigo de la ley.

Observamos que el Congreso Nacional -por lo menos en lo que a esta ley respecta- llevó a cabo una importante tarea de recopilación de normativa del derecho comparado y logró redactar un cuerpo normativo, abarcando las cuestiones más trascendentales a la par de los Estados más avanzados. Pero, nuevamente afirmamos, que el gran problema es que no se logra darle un estricto cumplimiento en lo fáctico.

Para ello, las empresas proveedoras de servicios de Internet deben contar con políticas más claras y sinceras respecto al tratamiento de datos personales de los usuarios.

Es necesario un serio compromiso por parte de las mismas, como así también la presencia de un Estado fuerte, a los fines de crear en la red un marco de seguridad jurídica que permita la concreción de negocios, el esparcimiento y cualquier otro tipo de tarea, sin perjuicios morales ni patrimoniales hacia usuario o cliente.

Finalmente, podemos concluir afirmando que es imperioso, por el momento, en el orden interno, la transformación en ley de varios proyectos legislativos, como por ejemplo, la regulación del envío de spams y el correo electrónico, entre otros.

Y por último, enfatizar en la consolidación de un bloque regional que regule las cuestiones referidas a Internet y a las nuevas tecnologías, de manera que los Estados, en conjunto, puedan encontrar las soluciones a la problemática que este medio masivo de información y comunicación acarrea.

[1] PIERINI, Alicia - TOMABENE, María Inés - LORENCES, Valentín. "Habeas Data. Derecho a la intimidad". LA LEY 18/06/2003. 7 - LA LEY 2003-D, 1482.
[2] "Ibídem".
[3] Art. 19 CN.- *"Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados…".*
[4] SAGÜÉS, Pedro Néstor, "Elementos de Derecho Constitucional" - Tomo 2. Edición actualizada y ampliada. Edit. Astrea. Buenos Aires. Año 1997. Pág. 383.
[5] "Ibídem".
[6] SANTOS BRIZ, Jaime, "Derecho de Daños", Madrid, 1963, pág. 196.
[7] "Ibídem".
[8] "Ibídem".
[9] "Ibídem".
[10] GARCÍA SAN MARTÍN, Luis. "Estudios Sobre el Derecho a la Intimidad". Buenos Aires, Edit. Paidós. 1995. Pág. 120.
[11] "Ibídem".
[12] En: "D.G.I. c/ Colegio Público de Abogados de la Capital Federal".
[13] MOEYKENS, Federico Rafael. "La Protección de Datos Personales en el Proyecto de Código Civil Unificado de Comercio de la República Argentina". [Revista en línea]. Año 2000. Junio. N° 023. Disponible desde: URL: http: //www.alfa-redi.org
[i] "Ibídem".
[15] "Ibídem".
[16] "Ibídem".
[17] "Ibídem".
[18] "Ibídem".
[19] SAGÜÉS, Pedro Néstor, Op. Cit, pág. 384
[20] "Ibídem".
[21] "Ibídem".
[22] Art. 18 CN.- *"…El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados…".-*
[23] En el caso ″Ponzetti de Balbín vs. Editorial Atlántida″ – (CSJN, 11/12/83).
[24] B.O., 25-X-1974.
[25] Art. 1071 bis Código Civil.- "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". (Artículo incorporado por art. 1° de la *Ley N° 21.173* B.O. 22/10/1975.)
[26] Art. 43 CN.- *"…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 aquéllos. No podrá afectarse el secreto de las fuentes de información periodística…".*
[27] *Art. 75.- "Corresponde al Congreso:*
"…22. Aprobar o desechar tratados concluidos con las demás naciones y con las organizaciones internacionales y los concordatos con la Santa Sede. Los tratados y concordatos tienen jerarquía superior a las leyes.
La Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo; la Convención sobre la Prevención y la Sanción del Delito de Genocidio; la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial; la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer; la Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes; la Convención sobre los Derechos del Niño; en las condiciones de su vigencia, tienen jerarquía constitucional, no derogan artículo alguno de la primera parte de esta Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos. Sólo podrán

ser denunciados, en su caso, por el Poder Ejecutivo nacional, previa aprobación de las dos terceras partes de la totalidad de los miembros de cada Cámara.
Los demás tratados y convenciones sobre derechos humanos, luego de ser aprobados por el Congreso, requerirán del voto de las dos terceras partes de la totalidad de los miembros de cada Cámara para gozar de la jerarquía constitucional…".

[28] SAGÜÉS, Pedro Néstor, Op. Cit, pág. 402.-

[29] "Ibídem".

[30] "Ibídem". Pág. 403.

[31] "Ibídem". Pág. 404.

[32] RIBAS ALEJANDRO, Javier; "Aspectos Jurídicos del Comercio Electrónico en Internet", página 50, Editorial Aranzadi, Navarra, España, 1999.

[33] "Ibídem". Pág. 50.

[34] "Ibídem". Pág. 50.

[35] "Ibídem". Pág. 51.

[36] VANOSSI, Jorge R., "El habeas data: no puede ni debe contraponerse a la libertad de los medios de prensa", ED, 159-948.

[37] BIANCHI, Alberto B., "Habeas data y derecho a la privacidad", ED 161-866.

[38] "Ibídem".

[39] RAVINOVICH-BERKMAN Ricardo David, "Cuestiones actuales en derechos personalísimos". págs. 135 y sigtes. Dunken. 1997.

[40] "Ibídem". Pág. 148.

[41] MOLINA QUIROGA, Eduardo, "Autodeterminación informativa y habeas data", JA 2/4/97.

[42] "Ibídem".

[43] "Ibídem".

[44] CIFUENTES, Santos; "Derechos Personalísimos", p. 166, Ed. Astrea 2a. ed., 1995.

[45] PARELLADA, Carlos A. "Daños en la actividad judicial e informática desde la responsabilidad profesional", págs. 222 y sgtes., Ed. Astrea 1990.

[46] Fuente: http://adrruiz.blogspot.com/

[47] "Ibídem".

[48] En Argentina es posible, con una simpleza que verdaderamente aterra, averiguar datos personales de otras personas. Todos los sitios que se nombran se tratan de páginas públicas, es decir que para ingresar no es necesario ningún tipo de identificación previa. Estos son algunos de los tantos ejemplos:

* *CUIL ó DNI a partir del nombre completo y provincia donde vive una persona:*
http://www.datosvirtuales.com/riesgo_crediticio/index_rc.php
* *CUIL y Nombre a partir de una patente:*
http://deudasrentas.cba.gov.ar/cedulones_ven.html
* *CUIL y Nombre a partir del DNI:*
http://www.anses.gov.ar/autopista/Serv_publicos/ooss.htm
* *Para saber si el CUIL también es un CUIT:*
http://seti.afip.gov.ar/padron-puc-constancia-Internet/ConsultaConstanciaAction.do
* *Fecha de Nacimiento, Nombre y Sexo a partir del CUIL:*
http://www.anses.gov.ar/servicios/yk2
* *Constancia de CUIL a partir del DNI, Fecha de Nacimiento y Sexo:*
http://www.anses.gov.ar/Autopista/Servpublicos/Cuil.htm
* *Informe financiero consolidado (importe de deuda con bancos / tarjetas), y cheques rechazados (para personas reales y jurídicas) a partir del CUIL:*
http://www.bcra.gov.ar/cenries/cr010000.asp
* *La AFJP a partir del CUIL:*
http://www.safjp.gov.ar/SISAFJP/popUpConultaAFJP.aspx
* *La historia laboral, obra social, datos personales (fecha de nacimiento, nombre completo), etc. a partir del CUIL:*
http://www.anses.gov.ar/autopista/Serv_publicos/historia.htm
* *Resumen de Situación Previsional (Aportes de seguridad social y obra social, contribución patronal):*
http://www.afip.gov.ar/misaportes
* *Teléfono fijo a partir del Apellido y Provincia (o viceversa):*

http://www.paginasamarillas.com.ar/home_blancas.asp
Por tan sólo 5 U$D uno puede averiguar el estado financiero detallado de una persona o sociedad argentina, ingresando a:
http://www.veraz.com.ar
http://www.datosvirtuales.com
http://www.decidir.com.ar
http://www.globinfo.com.ar
http://www.fidelitas.com.ar

[49] Fuente: URL: http://www.jus.gov.ar/datospersonales

[50] Art. 31 LPDP.- ARTICULO 31. — (Sanciones administrativas).
1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.
2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

[51] Fuente: URL: http://www.jus.gov.ar/datospersonales

[52] "Ibídem"

[53] "Ibídem".

[54] "Ibídem".

[55] CAMPANELLA DE RIZZI, Elena y STODART DE SASIM, Ana María, "Derecho a la intimidad e informática", La Ley 1984-B, 667.-

[56] "Ibídem".

[57] CIFUENTES, Santos; Op. Cit. pág. 186.-

[58] RABINOVICH-BERKMAN Op. Cit. págs. 164 a 167.-

[59] ARTICULO 2° — (Definiciones). *"A los fines de la presente ley se entiende por:*
— 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 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".

[60] ARTICULO 1° — (Objeto). "*La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos 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, así como también el acceso a la información*

que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.
En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas".
[61] Disponible en: URL: http://www.jus.gov.ar/datospersonales
[62] TRAVIESO, Juan Antonio - SEGURA, Pablo. "El registro nacional de bases de datos: herramienta para consolidar la cultura de la protección de datos". Publicado en: Sup. Act. 07/02/2006.
[63] "Ibídem".
[64] "Ibídem".
[65] "Ibídem".
[66] ARTICULO 21. — (Registro de archivos de datos. Inscripción).
"1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control..."
[67] TRAVIESO, Juan Antonio; Op. Cit.
[68] ARTICULO 7° — (Categoría de datos).
"1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas".
[69] LPDP. ARTICULO 2°; Op. Cit.
[70] PEYRANO, Guillermo F., "Régimen Legal de los Datos Personales y Habeas Data", Lexis Nexis, Depalma, 2002, p. 35 y sigtes. y 97 y sigtes.
[71] "Ibídem".
[72] "Ibídem".
[73] ARTICULO 6° — (Información).
"Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:
a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos".
[74] ARTICULO 4° — (Calidad de los datos).
"1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados".

[75] LPDP. ARTICULO 7°; op. Cit.

[76] LPDP. ARTICULO 2°; op. Cit.

[77] ARTICULO 11. — (Cesión).
"1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con 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.
2. El consentimiento para la cesión es revocable.
3. El consentimiento no es exigido cuando:
a) Así lo disponga una ley;
b) En los supuestos previstos en el artículo 5° inciso 2;
c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;
d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;
e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.
4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".

[78] ARTICULO 28. — (Archivos, registros o bancos de datos relativos a encuestas).
"1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.
2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna".

[79] C.Civ. y Com., San Isidro, sala 1ª, 21/06/96 -, Depaolini, Angela M. v. Organización Veraz, LLBA, 1996-1082.

[80] TRAVIESO, Juan Antonio – RUIZ MARTÍNEZ, Esteban. "La protección de datos personales de y los informes crediticios". LA LEY 31/08/2006.

[81] "Ibídem".

[82] "Tratándose de datos relativos a la historia crediticia resulta de particular interés para su titular, no ya por motivos que hacen a la protección de bienes jurídicos inmateriales como el honor o la intimidad, sino porque estos datos tienen la finalidad específica de servir para la adopción de decisiones en el mercado del crédito, en el cual una historia negativa cierra las puertas de acceso al sistema (Cfr. GILS CARBO, Alejandra "Régimen Legal de las Bases de Datos y Hábeas Data", Buenos Aires, Ed. LA LEY, 2001, p. 150 y sigtes.). (...) Ya lo decía el célebre jurista Ihering 'Permítasenos aducir un tercer ejemplo: el del comerciante. El crédito es para él, lo que el honor es para el militar, y lo que la propiedad es para el campesino; debe mantenerlo porque es la condición de su vida. El que le acusara de no tener cumplidas todas sus obligaciones y llenos sus compromisos, le lastimaría más sensiblemente que si le atacase en su personalidad o en su propiedad, mientras que el militar se reiría de esa acusación y el campesino la sentiría bien poco'" (VON IHERING, R. "La Lucha por el Derecho", trad. por Adolfo Posada, Ed. Araujo, Buenos Aires, p. 81). Dictamen doctora Alejandra Gils Carbó en el expte. 89.078, Juz. 13, Sec. 25, Cám. 34.621/05, "Mercobank S.A. s/liquidación judicial s/revisión por Tomada Jorge".

[83] "Ibídem".

[84] "Ibídem".

[85] "Las organizaciones de datos comerciales funcionan como una virtual inhabilitación o como una sanción, fundamentalmente al pequeño y mediano comerciante, lo cual implica separarlo, alejarlo o excluirlo de la cadena de crédito" (Juz. Cont. Adm. Fed. N° 7, Sec. 13, "Ozan, María Brígida c. Banco Central de la Republica Argentina s/hábeas data", 28/02/2003) (obtenido en www.protecciondedatos.com.ar).

[86] "Si bien es cierto que el responsable del tratamiento de datos — esto es, la persona física o de existencia ideal que es titular de un archivo o registro, base o banco de datos— tiene una obligación personal o directa de preservar la calidad de los que almacena y por tal razón debe realizar las diligencias apropiadas y exigibles — v. gr. verificar la exactitud y actualidad de la información— , carece de facultades para modificar, revisar o alterar la información que le fue suministrada por fuentes oficiales o por un tercero. Menos aun las tiene para dirimir las controversias que deben ventilarse y dirimirse en el Poder Judicial ante los tribunales competentes y por la vía pertinente" (CNCiv., sala G, "Montini, Roberto R. L. c. Diners Club Argentina SACT. s/hábeas data", 14/05/2003) (fuente: www.protecciondedatos.com.ar).

[87] TRAVIESO, Juan Antonio, "La experiencia argentina en materia de protección de datos personales: una visión institucional", Lexis Nexis, JA 2004-I, Fascículo N° 4, p. 85.

[88] "Ibídem".

[89] Al respecto cabe tener presente la siguiente jurisprudencia: CNCom., sala D, "Gago, Joaquín c. Batifora, María s/ejecución hipotecaria", DJ, 20-01-1999, p. 108, voto del Dr. Alberti: "Quien contrata con un inhabilitado no está autorizado para oponer, contra ese efecto legal inevitable de la situación de inhabilitación, su desconocimiento subjetivo de la calidad de inhabilitado que afectare a la persona con la cual contrató. El que esa inoponibilidad se produzca "a pesar" del invocado desconocimiento de la situación de inhabilitado que pesaba sobre el otro contratante, no es en modo alguno solución injusta, ni menos insuperable. Constituye carga de cada sujeto capaz, identificar al otro sujeto con el cual contrate, e informarse sobre la habilidad de derecho y de hecho de este otro sujeto; carga para cuya satisfacción el contratante capaz cuenta con un sistema de registros y de publicaciones, públicos y privados. Por tanto, no es invocable para derogar ese efecto legal imprescindible a la subsistencia del sistema de responsabilidad patrimonial — como en el caso alegó el accionante— , la ignorancia de que adoleciera el contratante capaz sobre la inhabilitación del otro contratante".

[90] Art. 42 de la Constitución Nacional: *"Los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos, a una información adecuada y veraz; a la libertad de elección y a condiciones de trato equitativo y digno. Las autoridades proveerán a la protección de esos derechos, a la educación para el consumo, a la defensa de la competencia contra toda forma de distorsión de los mercados, al control de los monopolios naturales y legales, al de la calidad y eficiencia de los servicios públicos, y a la constitución de asociaciones de consumidores y de usuarios. La legislación establecerá procedimientos eficaces para la prevención y solución de conflictos, y los marcos regulatorios de los servicios públicos de competencia nacional, previendo la necesaria participación de las asociaciones de consumidores y usuarios y de las provincias interesadas, en los organismos de control".*

[91] Cabe aquí mencionar la dudosa vigencia de la prohibición de informar dispuesta en la ley 25.065, por ser anterior a la ley 25.326 que regula igual materia en su art. 26. Al respecto, se encuentra pendiente de resolución en la CSJN la causa "Veraz c. Estado Nacional" donde el Procurador General de la Nación (doctor Nicolás Eduardo Becerra), en su dictamen, propone la derogación tácita por ser contraria a las disposiciones de la ley 25.326. La ley 25.065, en su art. 53 dispuso: "Prohibición de informar. Las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias tienen prohibido informar a las "bases de datos de antecedentes financieros personales" sobre los titulares y beneficiarios de extensiones de Tarjetas de Crédito u opciones cuando el titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina. Las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de Tarjetas de Crédito por las consecuencias de la información provista".

[92] ARTICULO 4° - LPDP; Op. Cit.

[93] ARTICULO 26. — (Prestación de servicios de información crediticia).

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.
4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.
5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

[94] GALLARDO, Roberto A. - LÓPEZ, Mario J. (h), "¿Existe la acción de hábeas data en la República Argentina?", nota a fallo, Cám. Nac. Crim. y Correc., sala de feria, 3/8/1997, "Ganora, Mario F. y otra"

[95] Algunos autores agregan como característica de los bancos públicos de datos, la de su "finalidad pública". Así, Gallardo y López señalan: "Esto indica que al menos existe una notoria diferencia entre las finalidades de los bancos: mientras que para los bancos de datos públicos la finalidad y la utilización única y excluyente debe ser pública, en el caso de los bancos privados éstas pueden o no ser públicas" (GALLARDO, Roberto A. - LÓPEZ, Mario J. [h], "¿Existe la acción de hábeas data...", cit., p. 237). Sin desconocer que la finalidad pública debe acompañar normalmente a los registros o archivos de datos públicos, la misma no constituye un elemento esencial para determinar su naturaleza, la que se deriva de la mera pertenencia a la organización estatal, aun ante la hipótesis de la existencia de un archivo de esa pertenencia cuya formación o existencia no responda a la finalidad pública que normalmente debe acompañarlos.

[96] En contra del criterio expresado, antes de la entrada en vigencia de la ley 25326 Ver Texto, se había resuelto que "la acción de hábeas data deducida con el objeto de requerir a la Dirección General Impositiva la información que posee respecto del actor, a fin de determinar la existencia de una actitud discriminatoria y persecutoria y, de ser así, ordenar la cesación de tales actos, es improcedente por no reunir aquélla la calidad de ente recolector y productor de información a terceros, conforme lo dispuesto en el art. 43 Ver Texto de la CN"

[97] ARTICULO 22. — (Archivos, registros o bancos de datos públicos).
"...3. En las disposiciones que se dicten para la supresión de los registros informatizados se esta blecerá el destino de los mismos o las medidas que se adopten para su destrucción".

[98] ARTICULO 24. — (Archivos, registros o bancos de datos privados).
"Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21".

[99] ARTICULO 21. — (Registro de archivos de datos. Inscripción).
1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.
2. El registro de archivos de datos debe comprender como mínimo la siguiente información:
a) Nombre y domicilio del responsable;
b) Características y finalidad del archivo;
c) Naturaleza de los datos personales contenidos en cada archivo;
d) Forma de recolección y actualización de datos;
e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
f) Modo de interrelacionar la información registrada;
g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
h) Tiempo de conservación de los datos;
i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.
El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

[100] ARTICULO 24. LPDP; Op. Cit.

[101] "Lo concreto es la existencia de una preocupación cada vez mayor por el destino que en definitiva pueden tener los datos personales almacenados en archivos, bases de datos, registros o ficheros, teniendo en cuenta la facilidad para su copia, transferencia y comunicación, incluso a

latitudes donde no existan restricciones ni niveles de protección adecuados para los mismos" (PEYRANO, Guillermo F.).-

[102] ARTICULO 1°. LPDP; Op. Cit.

[103] ARTICULO 21. LPDP; Op. Cit.

[104] GALLARDO, Roberto A. - LÓPEZ, Mario J. (h); Op. Cit., p. 239.-

[105] GRANERO, Horacio. "El impacto de las nuevas tecnologías en el Derecho". Artículo publicado por el Instituto de Informática Jurídica de la Universidad del Salvador. Disponible desde: URL: http://www.salvador.edu.ar/publicaciones

[106] "Ibídem".

[107] "Ibídem".

[108] "Ibídem".

[109] GRANERO, Horacio; Op. Cit.

[110] "Ibídem"

[111] GRAHAM Gart y Leslie Regan. "Retórica y realidad en las redes comunitarias canadienses", Publicado en Internet, Traducción de la cátedra Informática & Relaciones Sociales, Titular Emilio Cafassi, 1996, pág.1

[112] "Ibídem".

[113] "Ibídem".

[114] "Ibídem".

[115] Fuente: www.internetworldstats.com y Revista Newsweek Argentina.

[116] Estos son algunos datos para tener en cuenta:
En nuestro país, a diciembre de 2005 había 1.000.000 de internautas.
Desde el 2000 ha crecido 300% la cantidad de "conectados" a la red.
Aproximadamente 1 de cada 4 argentinos tiene acceso a la Red, eso es un 25% de la población. (Fuente: www.internetworldstats.com y Revista Newsweek Argentina).

[117] Aquí se puede observar cuales son las utilizaciones más frecuentes de Internet, refiriéndonos puntualmente a Argentina. A saber:
91% Para enviar mails.
91% Uso de buscadores.
82% Uso de chats.
84% Búsqueda de direcciones en mapas online.
79% Busca productos y servicios para comprar.
78% Se informa sobre el clima.
77% Busca información sobre sus hobbies.
73% Busca información sobre viajes.
68% Lee noticias. (Fuente: www.internetworldstats.com y Revista Newsweek Argentina).

[118] RIBAS ALEJANDRO, Javier; "Aspectos Jurídicos del Comercio Electrónico en Internet", página 50, Editorial Aranzadi, Navarra, España, 1999.

[119] "Ibídem".

[120] "Ibídem".

[121] Ver: "Vlex.com", "Noticias", de fecha 4 de Abril de 2001, "La Agencia de Protección de Datos multa con 20 millones a Terra por la fuga de datos personales de sus clientes el pasado mes de agosto. Disponible en: URL: //http://v2.vlex.com/vlex2/front/asp/noticias

[122] Ver: Diario "La Nación", de fecha 6 de Mayo de 2001, Sección "Cultura", página 13, donde el Director de Estudios en "l'Ecole des Hautes Etudes en Sciences Sociales de París", Roger Chartier, expone el peligro del "*analfabetismo tecnológico*".

[123] Ver: "DoubleClick sued for violating user's privacy rights (Suit seeks injunction that would require Company to cease using cookies without prior written consent of Internet Users)", publicado en "Tech Law",(http://www.lawnewsnetwork.com/stories/A15011-2000Feb2.html).
ver: PERINE, Keith; "Lawsuit says you can't escape Netscape (The latest lawsuit accusses America Online's subsidiary of illegally tracking web surfers)", publicado en "The Standard", de fecha 6 de Julio de 2000; http://www.thestandard.com/article/display/o,1151,16622,00html.

[124] Ver: "ElPais.es"; "El Senado de EE.UU. acusa al Gobierno de violar la intimidad de los internautas", nota de Javier del Pino, de fecha 18 de Abril de 2001.

[125] Todo ello, se ve avalado por las nuevas normativas incorporadas a nuestra Constitución Nacional, con la reforma de 1994.

[126] ARTICULO 5° — (Consentimiento).

". El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su 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.
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526".

[127] Agregando la ley que este consentimiento debe ser por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

[128] ARTICULO 4° — (Calidad de los datos).
"…2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley…".

[129] LLANEZA GONZALEZ, Paloma; "Internet y Comunicaciones Digitales (Régimen legal de las tecnologías de la información y la comunicación)", citado por Frene, Lisandro en LA LEY.-

[130] RIBAS ALEJANDRO, Javier; "Aspectos Jurídicos del Comercio Electrónico en Internet", página 52, Editorial Aranzadi, Navarra, España, 1999; citado por Frene, Lisandro en LA LEY.-

[131] "Ibídem".

[132] Información proporcionada por Spamhaus. Disponible desde: URL: http://www.spamhaus.com.

[133] Cuestión que puede ser experimentada diariamente pero sobre todo después del fin de semana.

[134] Como prueba de la ilegalidad de la gran mayoría de las bases de datos, bastaría con preguntarnos (en este mismo momento), cuántos de nosotros hemos dado nuestro "*consentimiento*" en forma "*libre*", "*expresa*", "*informada*" y "*por escrito*", de acuerdo a las pautas expresamente previstas en el Art. 5°, Inc.1°, de la Ley 25.326, para que nuestros 'datos personales' figuren en una 'base de datos' (en la cuales se van a sustentar -técnicamente- para el envío de "*spams*").

[135] ARTICULO 27. — (Archivos, registros o bancos de datos con fines de publicidad).
"1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo".

[136] ARTICULO 33. — (Procedencia).
1. La acción de protección de los datos personales o de hábeas data procederá:
a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.
ARTICULO 34. — (Legitimación activa).
La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.
Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.
En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.
ARTICULO 35. — (Legitimación pasiva).

La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

ARTICULO 36. — (Competencia).

Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Procederá la competencia federal:

a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y

b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

ARTICULO 37. — (Procedimiento aplicable).

La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

ARTICULO 38. — (Requisitos de la demanda).

1. La demanda deberá interponerse por escrito, 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.

En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.

2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate.

5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio.

ARTICULO 39. — (Trámite).

1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

ARTICULO 40. — (Confidencialidad de la información).

1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.

ARTICULO 41. — (Contestación del informe).

Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.

ARTICULO 42. — (Ampliación de la demanda).

Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

ARTICULO 43. — (Sentencia).
1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.
2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.
3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.
4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.
ARTICULO 44. — (Ambito de aplicación).
Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.
Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.
La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.
[137] ARTICULO 27. — (Archivos, registros o bancos de datos con fines de publicidad).
"…2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo".
[138] Disponible en: URL: http://www.lexisnexis.com.ar - Citar Lexis Nº 35003269.-
[139] Art. 18 CN; Op. Cit.-
[140] Art. 19 CN; Op. Cit.-
[141] Art. 11. CADH
"…2. 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 o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".
[142] *Art. 17 PIDCP – 1. "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".
[143] Art. 5 inc. 2 LPDP; Op. Cit.-
[144] "Ibídem".-
[145] Art. 1° LPDP; Op. Cit.-
[146] Art. 4 inc. 3° LPDP.- ARTICULO 4° — (Calidad de los datos).
"…3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención…"
[147] Art. 27 LPDP; Op. Cit.-
[148] "Ibídem".-
[149] Art. 1071 bis Código Civil; Op. Cit.-
[150] Tribunal Constitucional, España, sala 1, 8/11/1999, LL 2001-D-545.-
[151] Disponible en: URL: http://www.lexisnexis.com.ar - Citar Lexis Nº 35003269
[152] TANÚS, Gustavo Daniel. "El spam llegó a la justicia"; Artículo publicado en Information Technology, revista editada por Mind Opener S.A. Edición Nº 57 - Agosto 2001, pág. 90. Buenos Aires, Argentina.
[153] "Ibídem".-
[154] "Ibídem".-
[155] PALAZZI, Pablo A. "El hábeas data y el consentimiento para el tratamiento de datos personales".
[156] "Ibídem".-
[157] "Ibídem".-
[158] "Ibídem".-
[159] Respecto a esto, debemos expresar que en nuestro país existen diversos proyectos legislativos en torno a las nuevas tecnologías, a saber:
Correo Electrónico:
Anteproyecto de Ley de Protección del Correo Electrónico. Elaborado por la Secretaría de Comunicaciones.

Proyecto de Ley sobre Protección de las Direcciones Electrónicas. Elaborado por la Senadora Mirian Belen Curletti.

Protección de Datos:

Proyecto de Recomendación para considerar como Dato Sensible los Datos Personales de la Persona Menor de Edad. Elaborado por la Secretaría de Política Judicial y Asuntos Legislativos del Ministerio de Justicia de la Nación, a través de la Dirección Nacional de Protección de Datos Personales.

Proyecto de Ley para establecer el Derecho de todo consumidor y/o usuario de conocer su situación frente al riesgo crediticio y a requerir, en forma gratuita, la rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros, sean estos públicos o privados.

Proyecto de Comunicación solicitando la apertura en el interior del país de delegaciones regionales de la Dirección Nacional de Protección de Datos (D.N.P.D.P), elaborado por el Senador Marcelo Guinle.

Spam:

Anteproyecto de Ley de Regulación de las Comunicaciones Publicitarias por Correo Electrónico. Elaborado por la Secretaría de Comunicaciones.

Proyecto de Ley de "Prohibición de enviar o difundir en el territorio nacional publicidad a través del correo electrónico, salvo requerimiento del destinatario". Elaborado por la Diputada Nacional Bortolozzi de Bogado.

[160] Sancionada el 4/10/00, publicada en B.O. 2/11/00; decreto reglamentario N° 1558/01 del 3/12/01. Citado en: JUNVENT BAS, Francisco - FLORES, Fernando M. "La competencia federal o provincial en la acción de hábeas data". Publicado en: DJ 2004-3,310. La Ley. Disponible en: URL: //http://www.laley.com.ar.-

[161] SAGÜES, Néstor Pedro, "Derecho Procesal Constitucional. Acción de amparo", t. 3, p. 678, 4ª ed., Astrea, Buenos Aires, 1995. Citado en: JUNVENT BAS, Francisco - FLORES, Fernando M. Op. Cit.-

[162] BAZAN, Víctor, "El corpus data y sus peculiaridades frente al amparo", p. 218, Revista de Derecho Procesal, n° 4, Ed. Rubinzal-Culzoni, Santa Fe, 2000. Citado en: JUNVENT BAS, Francisco - FLORES, Fernando M. Op. Cit.-

[163] QUIROGA LAVIE-BENEDETTI-CENICACELAYA, "Derecho Constitucional Argentino", t. I, p. 612, Rubinzal Culzoni, Santa Fe, 2001. Citado en: JUNVENT BAS, Francisco - FLORES, Fernando M. Op. Cit.-

[164] CSJN, Fallos: 319:71.

[165] CSJN, "Ganora, Mario F. y otra", La Ley, 2000-A, 352.

[166] SAGÜÉS, Pedro Néstor. "Elementos de Derecho Constitucional" - Tomo 1. Edición actualizada y ampliada. Edit. Astrea. Buenos Aires. Año 1997. Pág. 256.

[167] BERGEL. Op. Cit., p. 210.

[168] Guastavino, Elías P., "Responsabilidad Civil y otros problemas jurídicos en computación", Bs. As., Ed. La Rocca, 1987, p. 136. Citado en: PALAZZI, Pablo A. "El hábeas data en la Constitución Nacional (La protección de la privacidad en la "era de la información")". Fuente: JA 1995-IV-710. Disponible em: URL: //http://www.lexisnexis.com.ar.-

[169] Conf. la opinión del citado autor en la Mesa Redonda sobre el tema "Impacto de la Reforma Constitucional en la actividad empresaria", 25/10/94, Universidad Argentina de la Empresa. Citado en: PALAZZI, Pablo A. Op. Cit.

[170] Conf. Ekmekdjian, Miguel A., "La garantía del `hábeas data' en el Proyecto de Ley de Unificación de la Legislación Civil y Comercial", en Revista Jurídica de Buenos Aires 1989-II-III, p. 72. Citado en: PALAZZI, Pablo A. Op. Cit.

[171] SAGÜÉS, Néstor P., "Amparo, Hábeas Data y Hábeas Corpus en la reforma constitucional", en LL 7/10/94. Citado en: PALAZZI, Pablo A. Op. Cit.

[172] BADENI, Gregorio, "Reforma Constitucional e Instituciones Políticas", Bs. As., Ad-Hoc, 1994, p. 247. Citado en: PALAZZI, Pablo A. Op. Cit.

[173] MASCIOTRA, Mario. "El Hábeas data. Garantía polifuncional". Publicado en: LA LEY 2005-D, 1511. Disponible en: URL: http:// www.laley.com.ar.-

[174] TRAVIESO, Juan A. "Garantías fundamentales de los derechos humanos", p 369, Buenos Aires, 1999. Citado en: Autor: CURIEL, Alicia I. "La protección de los datos personales. Análisis a la luz del derecho comparado". Publicado en: DJ 2004-4, 229. Disponible en: URL: http:// www.laley.com.ar.-

[175] RIVAS, Adolfo A., "Hábeas data", ponencia del autor en el XX Congreso Nacional de Derecho Procesal, San Martín de los Andes, del 5 al 9 de octubre de 1999, *Libro de Ponencias*, p. 340. Citado en: PEYRANO, Guillermo F. "Régimen legal de los datos personales y hábeas data". LexisNexis – Depalma. Año 2002. Disponible en: URL: http:// www.lexisnexis.com.ar.-

[176] "El hábeas data, dicen algunos, protege el derecho a la intimidad; pero al mismo tiempo, también se afirma que la defensa es de la privacidad, o de la dignidad humana, o el derecho a la información, o bien, la tutela del honor, o de la propia imagen o perfil personal, o el derecho a la identidad, o simplemente acotado a la autodeterminación informativa" (GOZAÍNI, Osvaldo A., "Introducción" a AA.VV., *La defensa de la intimidad y de los datos personales a través del hábeas data*, Ediar, Buenos Aires, 2001, p. 7). Citado en: PEYRANO, Guillermo F. Op. Cit.

[177] PALAZZI, Pablo A. "La defensa de la intimidad y de los datos personales a través del hábeas data". Ediar, Buenos Aires, 2001, p. 25. Citado en: PEYRANO, Guillermo F. Op. Cit.

[178] BIDART CAMPOS, Germán J., "¿Hábeas data, o qué? ¿Derecho a la verdad, o qué?", nota a fallo, LL, 1999-A-215. Citado en: PEYRANO, Guillermo F. Op. Cit.

[179] "Ibídem".-

[180] QUIROGA LAVIE-BENEDETTI-CENICACELAYA. Op. Cit.

[181] Art. 43 CN. Op. Cit.-

[182] QUIROGA LAVIE-BENEDETTI-CENICACELAYA. Op. Cit. Pàg. 613.-

[183] Art. 33 CN. (Procedencia).

"1. La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización".

[184] ARTICULO 34. — (Legitimación activa).

La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

[185] QUIROGA LAVIÉ, Humberto, ob. cit., p. 158. Citado en: PALAZZI, Pablo A. Op. Cit.

[186] SAGÜÉS, Néstor P., "Habeas Data: su desarrollo constitucional", en AAVV, Lecturas Andinas Constitucionales n. 3, Comisión Andina de Juristas, Perú, 1994. Citado en: PALAZZI, Pablo A. Op. Cit.

[187] GOZAÍNI, Osvaldo A., "El Habeas Data", en AAVV. Comentarios a la reforma constitucional, Asociación Argentina de Derecho Constitucional, 1995, p. 65. Citado en: PALAZZI, Pablo A. Op. Cit.

[188] Art. 43, 2º párrafo CN. "...Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización...".

[189] PUCCINELLI, Raúl O., "Habeas Data: aportes para una eventual reglamentación", ED 161-913. Citado en: PALAZZI, Pablo A. Op. Cit.

[190] Conf. la opinión de RIVERA, Julio C. Op. Cit. Citado en: PALAZZI, Pablo A. Op. Cit.

[191] PUCCINELLI, Raúl O., "Habeas Data: aportes para una eventual reglamentación", ED 161-913. Citado en: PALAZZI, Pablo A. Op. Cit.

[192] ARTICULO 35. — (Legitimación pasiva).

"La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes".

[193] Tal es la situación que contempla el art. 20 inc. 4 Ley Orgánica 5/92 del 29/10/92 de Regulación del Tratamiento automatizado de datos de carácter personal de España. Citado en: PALAZZI, Pablo A. Op. Cit.

[194] Como lo exigen las leyes que regulan los servicios de información crediticia en los Estados Unidos. Ver p. ej., la Fair Credit Reporting Act, 15 U.S.C., n. 1681ff. Citado en: PALAZZI, Pablo A. Op. Cit.

[195] BADENI, Gregorio, "Reforma Constitucional e Instituciones Políticas", Bs. As., Ad-Hoc, 1994, ps. 257 y 259. Citado en: PALAZZI, Pablo A. Op. Cit.
[196] GAIBROIS, Luis M., "El Habeas Data Argentino. La libertad informática es un derecho humano", en Revista de la Asociación de Magistrados y Funcionarios de la Justicia Nacional, n. 10, año VII, junio 1994, p. 26, quien cita el trabajo "Reclamo de Adepa a la Convención Constituyente", en Adepa, Noticiario de la Prensa Argentina,, n. 129, de julio 1994. Citado en: PALAZZI, Pablo A. Op. Cit.
[197] ARTICULO 14. — (Derecho de acceso).
"...2. 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 si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley...".
[198] JUNYENT BAS, Francisco - FLORES, Fernando M. La competencia federal o provincial en la acción de habeas data. Publicado en: DJ 2004-3, 310. Disponible en: URL: //http//: www.lexisnexis.com.ar.-
[199] "Ibídem".-
[200] Art. 38 LPDP.- (Requisitos de la demanda).
[201] ARTICULO 38, inc. 1º.- "1. La demanda deberá interponerse por escrito, 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.
En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen...".
[202] ARTICULO 21. — (Registro de archivos de datos. Inscripción).
"1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.
2. El registro de archivos de datos debe comprender como mínimo la siguiente información:
a) Nombre y domicilio del responsable;
b) Características y finalidad del archivo;
c) Naturaleza de los datos personales contenidos en cada archivo;
d) Forma de recolección y actualización de datos;
e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
f) Modo de interrelacionar la información registrada;
g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
h) Tiempo de conservación de los datos;
i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.
El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley"
[203] ARTICULO 38, inc. 1º - LPDP.- Op. Cit.-
[204] ARTICULO 38, inc. 2º - LPDP.- "...2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley...".
[205] Art. 14 LPDP.- Op. Cit.-
[206] Art. 16 LPDP.- (Derecho de rectificación, actualización o supresión).
"1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.
4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.
5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.
7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos".

[207] "Respecto de la carga probatoria, el art. 38, inc. 2º dispone que corresponde al afectado acreditar `los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley´ ". Citado en: PEYRANO, Guillermo F. Op. Cit.-

[208] ARTICULO 38, inc. 2º - LPDP.- Op. Cit.-

[209] ARTICULO 14 - LPDP.- Op. Cit.-

[210] ARTICULO 16 - LPDP.- Op. Cit.-

[211] "Es improcedente la acción de amparo iniciada para que la demandada, empresa dedicada a brindar informes sobre antecedentes comerciales, se abstenga de proporcionar información pues a tal fin es insuficiente la genérica manifestación del actor de verse impedido de tomar crédito, sin aportar elementos que permitan apreciar la seriedad de esa afirmación. Además, el hecho de no haber invocado la realización de gestiones previas y, en su caso, la inutilidad de éstas, impide también el acceso a la vía intentada" (Cám. Nac. Com., sala B, 4/7/1997). Citado en: PEYRANO, Guillermo F. Op. Cit.-

[212] Fallo de la Cámara Federal de Bahía Blanca, en el que se entendió "que no era imprescindible el reclamo administrativo previo requerido por el juez de grado..." (SERRA, María M., *El hábeas data...*, cit., p. 135). En similar, aunque incluso más amplio sentido, se propuso "recomendar que la acción de hábeas data, tanto contra una persona pública como privada, sea reglamentada, sin sujeción a ninguna vía administrativa previa y de manera autosuficiente, reglando los aspectos procesales necesarios, con la estructura de un proceso monitorio que contemple la implementación de medidas autosatisfactivas" (LEGUISAMÓN, Héctor E., "El hábeas data como medida autosatisfactiva en el marco de un proceso monitorio", ponencia del autor en el XX Congreso Nacional de Derecho Procesal, San Martín de los Andes, del 5 al 9 de octubre de 1999, *Libro de ponencias*, p. 330). Citado en: PEYRANO, Guillermo F. Op. Cit.-

[213] PUCCINELLI, Oscar R. "El hábeas data en el derecho constitucional latinoamericano". Publicado en: LA LEY 1997-D, 215. Disponible en: URL: //http//: www.lexis.nexis.com.ar.-

[214] SAGUES, Néstor P., "Subtipos de hábeas data", JA, 20/12/95, p. 31 y siguientes. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[215] "Ibídem".-

[216] "Ibídem".-

[217] En tal inteligencia, Bergel --citando a Roppo-- menciona que "En un cierto sentido (el derecho de inserción) es simétrico al derecho de cancelación y se funda en las circunstancias que los sujetos tienen un interés preciso en que los propios datos sean insertados en un determinado banco de datos que los omitió, insertar junto a otros datos suyos que pueden modificar su perfil o despejar dudas al respecto" (BERGEL, Salvador Darío, "El habeas data: instrumento protector de la privacidad", en "Revista de Derecho Privado y Comunitario", Nº 7, "Derecho privado en la reforma constitucional", Rubinzal Culzoni, Santa Fe, 1994. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[218] SAGÜÉS, Néstor P. Op. Cit. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[219] "Según la declaración sobre la regulación de datos personales automatizados, adoptada por la Asamblea General de la Organización de las Naciones Unidas en su 45ª sesión ordinaria bajo el nombre de "Directrices para la regulación de ficheros automáticos de datos personales" los datos sensibles son ciertos tipos de datos personales cuya utilización puede dar lugar a "discriminaciones ilegales o arbitrarias". Entre los datos que no deben ser recogidos se menciona explícitamente los

que hacen referencia a raza, origen étnico, color, vida sexual, opinión política, religión, filosofía y otras creencias, así como el ser miembro de asociaciones o uniones sindicales (parágr. 5).(Para un análisis más particularizado ver el trabajo de EKMEKDJIAN, Miguel A. y PIZZOLO, Calogero, "Habeas data. El derecho a la intimidad frente a la revolución informática", p. 43, Ed. Depalma, Buenos Aires, 1996. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[220] BERGEL, Salvador Darío, "El habeas data: instrumento protector de la privacidad", en "Revista de Derecho Privado y Comunitario", Nº 7, "Derecho privado en la reforma constitucional", p. 216, Ed. Rubinzal Culzoni, Santa Fe, 1994. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[221] PALAZZI, Pablo A., "El habeas data en la Constitución nacional. (La protección de la privacidad en la "era de la información") JA, 20/12/94, p. 14. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[222] En este sentido, advierte Palazzi, refiriéndose al caso argentino, que al no haber seguido nuestra Constitución el modelo de las reglamentaciones extranjeras, incurre en el error de sólo permitir actuar sobre los datos si existe falsedad o discriminación, cuando debiera haber contemplado otros supuestos (PALAZZI, Pablo A., "El habeas data en la Constitución nacional". (La protección de la privacidad en la "era de la información), JA, 20/12/94, p. 14). Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[223] VANOSSI, Jorge R., "El habeas data no puede ni debe contraponerse a la libertad de los medios de prensa", ED, 159-948. Citado en: PUCCINELLI, Oscar R. Op. Cit.-

[224] "Ibídem".-

[225] BAZÁN, Víctor. La protección de datos personales y el derecho de autodeterminación informativa en perspectiva de Derecho comparado. Publicado en: LLGran Cuyo 2005 (junio), 453. Disponible en: URL: //http//: www.laley.com.ar.-

[226] Otras fuentes dignas de mención en el marco comunitario de Europa, vgr., son: la Resolución del Parlamento Europeo sobre la protección de los derechos de la persona frente al avance de los progresos técnicos en el campo de la informática, de 1979; la Recomendación de la Comisión relativa al mencionado Convenio del Consejo de Europa para la protección de las personas con respecto al procesamiento automático de datos personales, de 1981; la Directiva 2002/58/CE (emitida por el Parlamento y el Consejo en fecha 12 de julio de 2002), relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Citado en: BAZÁN, Víctor. Op. Cit.-

[227] Cfr. PADILLA, Miguel M. "La Directiva 95/46/CE de la Unión Europea". Buenos Aires, Argentina: LA LEY, 16 de marzo de 1999, ps. 1/2. Citado en: BAZÁN, Víctor. Op. Cit.-

[228] "Ibídem".-

[229] "Ibídem".-

[230] CURIEL, Alicia I. "La protección de los datos personales. Análisis a la luz del derecho comparado". Publicado en: DJ 2004-4, 229. Disponible en: URL: //http:// www.laley.com.ar.-

[231] Art 1° Ley Orgánica 15/99 de Protección de Datos de Carácter Personal (B:O:E: 14-12-1999). Citado en: CURIEL, Alicia I.- Op. Cit.-

[232] El Convenio de Estrasburgo entró en vigor el 1° de octubre de 1985 de conformidad a su art. 22.2 (BOE núm 274 15 Nov. 1985) http://www.europa.eu.int/comm/internal_market. Citado por: CURIEL, Alicia I.- Op. Cit.-

[233] Véase www.europa.eu.int/comm/internal_market. Citado por: CURIEL, Alicia I.- Op. Cit.-

[234] Veáse www.usdoj.gov/oip/foia_updates. Citado por: CURIEL, Alicia I.- Op. Cit.-

[235] Confr. Constitución de Guatemala Art. 31. Citado por: CURIEL, Alicia I.- Op. Cit.-

[236] Confr. Constitución de Colombia Art. 15. Citado por: CURIEL, Alicia I.- Op. Cit.-

[237] Confr Constitución Rca Federativa del Brasil Arts. 5 y 77. Citado por: CURIEL, Alicia I.- Op. Cit.-

[238] Confr Constitución del Paraguay Arts. 135 y 126. Citado por: CURIEL, Alicia I.- Op. Cit.-

[239] Confr. Constitución del Perú Art. 200. Citado por: CURIEL, Alicia I.- Op. Cit.-

[240] Compendio de Acciones de Garantía Dpto. de Estudios Jurídicos Ed. San Marcos, Lima, 2003. Citado por: CURIEL, Alicia I.- Op. Cit.-

[241] Conforme ley 19.628 de 2000. Citado por: CURIEL, Alicia I.- Op. Cit.-

[242] Véase el texto Constitución de la Ciudad Autónoma de Buenos Aires. Citado por: CURIEL, Alicia I.- Op. Cit.-

[243] TRAVIESO, Juan Antonio - SEGURA, Pablo. Publicado en: Sup. Act. 07/02/2006, 1. Disponible en: URL://http//: www.laley.com.ar

[244] ARTICULO 1° LPDP. Op. Cit.-

[245] ARTICULO 28 LPDP. Op. Cit.-
[246] ARTICULO 2º LPDP. Op. Cit.-

BIBLIOGRAFÍA

a) General

SAGÜÉS, Pedro Néstor, "Elementos de Derecho Constitucional" - Tomos 1 y 2. Edición actualizada y ampliada. Edit. Astrea. Buenos Aires. Año 1997.-

TRAVIESO, Juan Antonio – SEGURA, Pablo. "El registro nacional de bases de datos: herramienta para consolidar la cultura de la protección de datos". Edit. La Ley.-

PUCCINELLI, Oscar R. "Tipos y subtipos de hábeas data en el derecho constitucional latinoamericano". Edit. La Ley.-

CURIEL, Alicia I. "La protección de los datos personales. Análisis a la luz del derecho comparado". Edit. La Ley.-

PALAZZI, Pablo A. "El hábeas data en la Constitución Nacional (la protección de la privacidad en la "era de la información")". Edit. Lexis Nexis - Abeledo Perrot.-

PUCCINELLI, Oscar R. "La obligación de la inscripción de las bases de datos privadas y públicas". Edit. La Ley.-

b) Especial

CIFUENTES, Santos. "Derecho personalísimo a los datos personales". Edit. La Ley. Año 1999.-

EKMEKDJIAN. "Tratado de derecho constitucional". Edit. Depalma. Año 1993.-

QUIROGA LAVIÉ-BENEDETTI-CIENCIACELAYA. "Derecho Constitucional Argentino". Edit. Rubinzal Culzoni. Santa Fe. Año 2001.-

PALAZZI, Pablo A. "El hábeas data y el derecho al olvido". JA, 1997-I 33.-

TRAVIESO, Juan Antonio-RUIZ MARTÍNEZ, Esteban. "La protección de datos personales y los informes crediticios". Edit. La Ley.-

BAZÁN, Víctor. "La protección de datos personales y el derecho de autodeterminación informativa". Edit. La Ley.-

PIERINI, Alicia - TORNABENE, María Inés - LORENCES, Valentina. "Hábeas data. Derecho a la intimidad". Edit. La Ley. Año 2003.-

PEYRANO, Guillermo F. “Régimen Legal de los Datos Personales y Hábeas Data”. Edit. Lexis Nexis - Depalma. Año 2002.-

CIFUENTES, Santos. “Derechos personalísimos”. Edit. Astrea. Año 1995.-

TRAVIESO, Juan Antonio-MORENO, María del Rosario. “La protección de los datos personales y de los sensibles en la ley 25.326”. Edit. La Ley.-

ÍNDICE

CAPÍTULO II

BASES DE DATOS

CAPÍTULO III

INTERNET Y LAS NUEVAS TECNOLOGÍAS

CAPÍTULO IV

HÁBEAS DATA

Pág.

CAPÍTULO V

ANÁLISIS DE LA LEY 25.326