UNIVERSIDAD AUSTRAL DE CHILE

Facultad de Ciencias Jurídicas y Sociales

Escuela de Derecho

LA PROTECCIÓN DE DATOS PERSONALES. OTRO ÁMBITO DE LA PROTECCIÓN A LA VIDA PRIVADA.

Profesor Patrocinante:

Sr. ALFONSO BANDA VERGARA

Postulantes:

MARIO ROMERO OBREQUE

EMILIANO SEGURA RAMÍREZ

Valdivia Chile 2009

Valdivia, 19 de Octubre de 2009

Señor ANDRES BORDALI SALAMANCA
Director Instituto Derecho Público
Presente

Señor Director:

Procedo a informar la Memoria de Prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales de la Universidad Austral de Chile, presentada por los estudiantes señores MARIO ROMERO OBREQUE y EMILIANO SEGURA RAMIREZ, intitulada ***"La protección de datos personales. Otro ámbito de la protección a la vida privada."***

Los autores postulan que la protección de datos personales no está necesariamente referida a si se debe contar con acopios de datos relativos a la vida privada, sino que más bien a que los que administran esas bases de datos lo hagan adecuadamente de manera que los titulares de éstos puedan controlarlos incluso incorporándose como derecho fundamental la autodeterminación informática.

Para este efecto, además de analizar el ámbito de lo que comprendería la vida privada, se avocan al estudio de la Ley sobre Protección de Datos Personales, N° 19.628, la cual no regula sino algunos aspectos del tema, y estiman que no otorga una garantía suficiente que proteja y evite los abusos que afectan la intimidad y los datos personales de millones de personas. Se destaca que, paradójicamente a su denominación, la ley primeramente se ocupa de la protección de las empresas administradoras de datos y no a sus titulares, es decir, protege más bien el "negocio" del tratamiento de datos. Por ello, plantean como hipótesis la cuestión de si la protección de datos por parte de la ley constituiría una promesa incumplida y cuáles podrían ser las soluciones al problema.

Con el fin de definir los diferentes tipos de datos y los distintos modelos de bases o bancos de datos se analizan normas del Derecho Comparado, partiendo de la "privacy" norteamericana, pasando por la "riservatezza" italiana, y llegando al derecho a la autodeterminación informativa como aporte interesante de la doctrina alemana. Se deja ver en nuestro sistema un vacío en cuanto no se ha abordado directamente por la ley el tema sobre la propiedad de la información dejando en cierto modo al titular de los datos en situación desmejorada frente a las poderosas empresas que se "apropian" de estos datos y los manejan en su beneficio. En los capítulos III y IV se analizan aspectos relevantes de la ley, tales como los derechos del titular de los datos, derechos de acceso, oposición, indemnización, la autoridad de control (Consejo para la Transparencia); y los mecanismos contemplados en la ley para el efecto, entre los cuales está una acción reconocida al titular –habeas data- para ejercerla contra el responsable de la base de datos y, en su caso, recurrir al Juez de letras con el propósito de hacer realidad sus derechos legalmente reconocidos.

Concluyen que en Chile no existe un desarrollo doctrinal adecuado sobre la materia y que la ley referida -19.628- es deficitaria y que tiende más bien a legitimar la comercialización de datos de millones de personas por parte de las empresas del rubro antes de dar una debida protección a los titulares de dichos datos y ello debido fundamentalmente a que la ley no encara el problema de la propiedad de los datos permitiendo que las empresa los hagan suyos como cosas disponibles para ser apropiadas por cualquiera. Con ello dejan en claro los tesistas que se pierde el objetivo principal que debió asumir la ley, de dar protección a la vida privada de las personas. Postulan los autores la consagración constitucional del derecho a la autodeterminación informativa y dar rango constitucional a la acción de habeas data, para así subsanar las deficiencias de la ley de manera que rija en Chile, efectivamente, el derecho a la protección de la vida privada de las personas.

En conclusión la Memoria constituye, en opinión del informante, un efectivo e interesante aporte al estudio de este tema de enorme trascendencia y actualidad y, por ello, merece la aprobación del profesor que suscribe quien, para todos los efectos reglamentarios la evalúa con nota 6.0 (seis punto cero). Sin otro particular, le saluda muy atentamente al señor Director,

ALFONSO BANDA VERGARA
Profesor de Derecho Constitucional

INDICE

INTRODUCCIÓN.-

Los derechos fundamentales según como hoy los conocemos surgieron a principios del siglo XVIII; la semilla fue sembrada por los movimientos independentistas de las colonias inglesas en Norteamérica y por la Revolución Francesa. Sin embargo, estos dos hechos históricos no aludieron en sus reivindicaciones a la protección a la vida privada por no existir en aquel tiempo reales amenazas que merecieren la imposición de medidas especiales, vale decir, este derecho no formó parte de la primera generación de libertades que fueron exigidas a los detentadores del poder político de aquel tiempo.[1]

En la segunda mitad del siglo XIX, con el desarrollo de tecnologías capaces de capturar imágenes y de efectuar comunicaciones a la larga distancia (fotografía y telégrafo) comenzó a tomar fuerza la discusión en torno a la protección de la vida privada contra intromisiones no autorizadas por parte de terceros.

Un momento determinante en esta evolución fue la aparición del célebre artículo titulado "*Right to Privacy"*, publicado en 1890 en la *Harvard Law Review.* Dicho trabajo, obra de los juristas *Louis Brandeais* y *Samuel Warren*, marcó el inicio de la discusión sobre lo que para el mundo anglosajón es el derecho a la privacidad, y que para países como los nuestros, más vinculados a la tradición jurídica de Europa continental sería el derecho a la vida privada o el derecho a la intimidad. Su desarrollo estuvo ligado al gran auge que tuvo en Norteamérica desde finales del siglo XIX y hasta hoy la actividad periodística, esto potenciado por el nacimiento de los principales medios de información escritos de Estados Unidos como el Washintong Post o el New York Times. La aparición de tales medios, irrumpiendo en la intimidad de políticos, artistas y personas con figuración social hizo necesario el desarrollo de una contención a los abusos que en nombre de la libertad de expresión se estaban cometiendo.

---

[1] La división de los derechos humanos en tres generaciones fue concebida por primera vez por Karel Vasak en 1979. Cada una se asocia a uno de los grandes valores proclamados en la Revolución Francesa: libertad, igualdad, fraternidad. **Los derechos de primera generación** son los derechos civiles y políticos, vinculados con el principio de libertad. Generalmente se consideran derechos de defensa o negativos, que exigen de los poderes públicos su inhibición y no injerencia en la esfera privada. Por su parte, **los derechos de segunda generación** son los derechos económicos, sociales y culturales, que están vinculados con el principio de igualdad. Exigen para su realización efectiva de la intervención de los poderes públicos, a través de prestaciones y servicios públicos. Existe cierta contradicción entre los derechos contra el Estado (primera generación) y los derechos sobre el Estado (segunda generación). Los defensores de los derechos civiles y políticos califican frecuentemente a los derechos económicos, sociales y culturales como falsos derechos, ya que el Estado no puede satisfacerlos más que imponiendo a otros su realización, lo que para éstos supondría una violación de derechos de primera generación. Finalmente, **la tercera generación de derechos**, surgida en la doctrina en los años 1980, se vincula con la solidaridad. Los unifica su incidencia en la vida de todos, a escala universal, por lo que precisan para su realización una serie de esfuerzos y cooperaciones en un nivel planetario. Normalmente se incluyen en ella derechos heterogéneos como el derecho a la paz, a la calidad de vida o las garantías frente a la manipulación genética, aunque diferentes juristas asocian estos derechos a otras generaciones: por ejemplo, mientras que para Vallespín Pérez la protección contra la manipulación genética sería un derecho de cuarta generación, para Roberto González Álvarez es una manifestación, ante nuevas amenazas, de derechos de primera generación como el derecho a la vida, la libertad y la integridad física.

En el presente el gran desafío para la protección de la vida privada viene dado por el enorme desarrollo de la tecnología, sobre todo de la informática, con la que se puede vigilar, interferir o asegurar cada ámbito de la vida moderna, lo que unido a la creación de grandes bases de datos que contienen todo tipo de información respecto de antecedentes personales, comerciales e incluso familiares de un individuo, parecieran conspirar contra un ámbito mínimo de privacidad al que toda persona puede legítimamente aspirar, ámbito el cual es considerado por algunos como un derecho humano equiparable a la vida y a la libertad personal, todo lo cual ha hecho necesario legislar con respecto a las telecomunicaciones o al uso de la informática, ello por cuanto existe la posibilidad técnica de proteger, compartir o difundir una masa de información que nunca antes había estado al alcance de todas las personas.

La creación de grandes bases de datos personales se encuentra totalmente justificada en el mundo moderno, toda vez que la información que ellas contienen hacen posible la toma de decisiones por parte de la autoridad gubernamental en los más diversos ámbitos (políticas medioambientales, de control financiero, tributario, policiales, inmigratorios, aduaneros, de control demográfico, etc.). Lo mismo en el caso de la empresa privada, la necesidad de contar con información completa, sectorizada y actualizada, es una poderosa herramienta en la implementación de estrategias de comercialización, volúmenes de producción, lugares y sectores en donde invertir, etc. De esta forma, la problemática actual no está dada por la pregunta de si es o no necesario contar con acopios de datos referentes a aspectos de la vida privada de las personas, sino en la obligación de cada uno de los administradores de estas bases de datos de no darle el tratamiento de bienes mostrencos, esto es, un bien sin dueño que se compra y vende al margen de la voluntad de los titulares de los datos que contienen. Esto significa que nosotros, los titulares, sepamos en manos de quién o de quiénes se encuentra la información que atañe a nuestra situación patrimonial, vida familiar, hábitos de vida, gustos, en fin la amplia gama de aspectos que forman nuestra cotidianeidad, y junto a ello poder exigir que tal información no salga de nuestro control y poder decidir respecto al destino que se le dará a tales antecedentes o, por lo menos, poder imponernos siempre de su ubicación.

Se ha dicho que "el abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la intimidad, porque detentándose un enorme cúmulo de datos y cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados. Esta imagen inmaterial debe ser resguardada porque puede ser creada errada o dolosamente y sólo con fines de lucro, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio".[2]

[2] Artículo innominado aparecido en el sitio web www.habeasdata.org, en julio de 2008.

Estamos en el contexto de un conflicto que se presenta entre dos garantías individuales y de rango constitucional. A saber, por un lado el derecho a la intimidad, y por otro el derecho ejercer una actividad lícita, como es el tratamiento de datos personales.

En cuanto a qué entender por intimidad, existen posturas que casi podríamos decir que son antagónicas. Para algunos es una creación del Estado mediante la ley, es decir se configura por un acto de autoridad.[3] Eso implica que puede modificarse y que, en cada caso, debe darse una justificación, o sea debe explicarse por qué razón esa materia no es objeto de interés público de modo que los particulares pueden decidir al respecto con entera libertad. Para otros la protección a la vida privada, el respeto a la intimidad, son derechos humanos equiparables a la libertad personal y a la seguridad individual, por ende anteriores y superiores al ordenamiento jurídico positivo, por lo que este ordenamiento sólo debe reconocerlos y regular su ejercicio.

Sea cual sea la opción que se tome con respecto a la génesis de estos derechos el punto a clarificar es cuáles son los espacios o esferas que consideraremos dentro de lo público o privado; para los efectos de este trabajo, qué datos son de carácter privado y cuales podríamos considerar del libre acceso de quién se interese en averiguarlos. Una distinción entre privacidad e intimidad se hace, para efectos de metodología, algo indispensable. Por otra parte, ninguna decisión, ningún espacio es absolutamente privado en el sentido de estar por completo, en todo momento, bajo todo punto de vista fuera del escrutinio público. La función de la ley es restringir y delimitar las circunstancias en que está justificada la intervención, ya sea de la autoridad estatal, ya sea de particulares. Por ejemplo, lo que cada quien decide hacer en su domicilio es asunto privado o la forma en que cada quien decida organizar su vida familiar es asunto privado, a menos que haya violencia: en ese caso, para proteger a las víctimas de maltrato, la autoridad tiene el derecho y la obligación de intervenir, situación que motivó la entrada en vigor de Ley Nº 19.325, la primera Ley de Violencia Intrafamiliar en Chile.

Todas estas consideraciones motivaron la dictación de la Ley N° 19.628, ley que tuvo su origen en una moción presentada ante el Senado con fecha 5 de enero de 1993, y tenía por propósito llenar un vacío manifiesto en el ordenamiento jurídico chileno mediante el otorgamiento de una adecuada protección al derecho de la vida privada de las personas ante eventuales intromisiones ilegitimas. Este objetivo tan ambicioso motivó que el texto fuera sometido a largas discusiones y cambios en cada uno de los trámites constitucionales que debió superar tanto ante el Senado como en la Cámara de Diputados. Finalmente, y con el objeto de superar las divergencias entre el Senado y la Cámara de Diputados, se formó una Comisión Mixta integrada por miembros de cada una de las cámaras.

[3] Escalante Gonzalbo Fernando, "El Derecho a la Privacidad", Instituto Federal de Acceso a la Información Pública, México, año 2004.

El texto aprobado se limitó a regular uno de los aspectos de la protección de la vida privada, como lo es el tratamiento que los organismos públicos y los particulares efectúen de los datos de carácter personal almacenados en registros o bancos de datos sean estos de carácter automatizado o no. La aspiración de regular el fenómeno de la protección de la vida privada como un todo, tuvo una vez más que ser pospuesta. Este es el motivo por el cual la Ley se denomina "Sobre Protección de la Vida Privada", cuando realmente sólo regula un aspecto de tal importante materia.

Si bien en el proyecto original se tomaron como parámetros orientadores los principales criterios esbozados por el derecho comparado y los tratados y convenciones internacionales, pareciera ser que a medida que la discusión de la Ley se fue desarrollando, la injerencia de la derogada Ley Orgánica española de 29 de octubre de 1992, Sobre Regulación de Tratamiento Automatizado de Datos, fue cada vez mayor.

La ley 19.628 sobre protección a la vida privada, que fue constantemente postergada debido a las presiones efectuadas por diversos sectores, vino a llenar un vacío legislativo que a lo menos debió ser satisfecho 10 años antes de su entrada en vigencia. Dichas tensiones, que rodearon su tramitación legislativa, se manifiestan con fuerza en algunos temas delicados como es el tema de la propiedad de los datos, tema que abordaremos en el Capítulo II de este trabajo.

Como una primera aproximación a esta materia debemos decir que el vacío destinado a llenar por la ley sólo lo ha sido en parte y de manera imperfecta, toda vez que como dijimos al comienzo se utilizó como modelo una normativa europea que ya había sido superada en el momento que fue tomada como referencia. Como muestra de esta imperfección tenemos la noticia que suministraron hace un tiempo algunos medios de comunicación referente a que en Internet se estaban transando bases de datos con antecedentes personales de más de seis millones de chilenos, sin su consentimiento; ello es un reflejo palmario que esta realidad está golpeando con fuerza a nuestra puerta y poniendo a prueba a la legislación en este aspecto.[4]

La situación descrita anteriormente, así como otras similares, nos llevan a pensar que nuestra legislación actual sobre protección a la vida privada y a los datos de carácter personal, Ley Nº 19.628, no es salvaguarda suficiente para evitar abusos e intromisiones en la intimidad y los datos personales, que se trata de una normativa deficitaria a la cual hay que introducir rectificaciones, ya que como producto legal siempre será superado por la realidad.

Sobre este punto hemos de señalar que la discusión parlamentaria que rodeó a la tramitación de la ley estuvo muy contaminada por factores exógenos que en lugar de

[4] Noticia aparecida en el la edición El Mercurio on line, Domingo 11 de Mayo, 2008.

enriquecer el debate legislativo ayudaron a empobrecerlo. En efecto, durante la tramitación del proyecto de ley que concluyó con la dictación de la Ley N° 19.628 se observa la influencia de un lobby ejercido sin ambages por las empresas y organismos particulares que a la época administraban las bases de datos con información de personas naturales. Este lobby castró en gran medida lo que podría haber sido una legislación moderna y que efectivamente cumpliera con la finalidad que prometía, esto es, proteger los derechos de los titulares de datos de los posibles abusos que se cometieran durante el proceso de recogida y tratamiento de sus datos personales.

Como ejemplo de lo expuesto anteriormente podemos mencionar algo que para la doctrina ha resultado toda una paradoja, que el primer derecho consagrado en la ley resulta ser el que tiene toda persona para efectuar el tratamiento de datos personales. Resulta muy contradictorio que la ley comience protegiendo en su art.1° a aquellos que en teoría resultan ser la parte fuerte de la relación jurídica, las empresas administradoras de datos y no a quien se supone es la parte más débil en dicha relación, los titulares de datos.

La influencia de este lobby, unido al poco conocimiento que del tema demostraron tener nuestros legisladores dio como resultado un producto normativo de sólo regular factura, más preocupado de regularizar y amparar el negocio de tratamiento de datos personales por parte de empresas dedicadas a dicha actividad que de ser un verdadero amparo para los titulares de datos que sientan que su intimidad está siendo conculcada.

Por lo señalado estimamos que nuestra legislación en materia de protección de datos personales debe ser revisada a la brevedad, actualizándola y librándola de los ripios que en su génesis se manifestaron. Nos planteamos como objetivo del presente trabajo dar una visión de amplio espectro sobre el tema de la protección de datos (evolución de ciertos conceptos como autodeterminación informativa, habeas data y otros), para posteriormente aterrizar en nuestra legislación y ver en concreto que la protección efectiva de los datos personales es una promesa aún incumplida, para finalizar haremos un análisis de las posibles soluciones que se han dado al respecto. A fin de cumplir con los objetivos planteados dividiremos el presente estudio en cinco capítulos:

En el capítulo primero veremos el núcleo del sistema, los datos personales. La definición que da nuestra ley sobre el punto, que ha sido catalogada por la doctrina como acertada. También haremos un esbozo de sus tipos y clases.

En el capítulo segundo estudiaremos la propiedad de la información. Aquí haremos mención a un tema que nuestra ley no abordó de manera directa y que ha suscitado controversia, este es el tema de la propiedad de los datos, a quién pertenecen los mismos, señalaremos la opinión de algunos destacados tratadistas y manifestaremos cuáles son las tendencias que en derecho comparado se siguen.

En el capítulo tercero revisaremos los principales aspectos de la Ley N° 19.628, su ámbito de aplicación, principios que la rigen, principales derechos que se consagran, reglamento, así como la reciente autoridad de control creada por la ley de acceso a la información: El Consejo para la Transparencia.

En el capítulo cuarto analizaremos la protección de datos personales. Aquí veremos los mecanismos que nuestra ley consagra para cautelar la protección de datos, ello nos llevará a analizar el instrumento del Habeas Data.

Finalmente en el capítulo quinto expondremos las conclusiones finales a las que hemos arribado con este trabajo, así como también expondremos algunas ideas señaladas por nuestra doctrina para reforzar la precaria arquitectura legal de nuestro ordenamiento jurídico en esta materia.

CAPÍTULO I: LOS DATOS DE CARÁCTER PERSONAL.

Comenzaremos este trabajo analizando el elemento básico objeto de protección legal, cual es el llamado dato, el núcleo base de todo el sistema. Veremos algunos conceptos y esquematizaciones.

1.- Determinación del vocablo "dato".

El objeto último de protección son los datos de carácter personal. Conceptualmente, un dato es un antecedente que da cuenta de un hecho o de una característica determinada. El conjunto organizado de datos constituyen información y, sociológicamente hablando, un nuevo bien económico de alto valor y una forma de poder.[5]

Un dato es personal o nominativo cuando permite identificar cualquier característica de una persona para relacionarse en sociedad, por ejemplo al consignarse en una guía de teléfonos datos generales o cuando son de mayor importancia o sensibilidad como ocurre con la filiación política, el credo religioso que se profesa, los antecedentes laborales, la situación de salud, la mayor o menor riqueza, etc.

2.- Las Bases o Bancos de Datos.

Nuestra Ley N° 19.628 entiende como **registro** o **base de datos** a "*un conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos".*

Se ha criticado la sinonimia que hace la ley entre las expresiones registro y base de datos, ya que la voz "registros" denota un conjunto organizado de datos de carácter personal, en cambio los "bancos de datos" imponen un concepto más especializado que comprende a un fondo común de datos, característica que comparte con los registros, pero que se diferencia de ellos porque son accesibles a varios usuarios. Es en este último sentido en el que parecen haber sido tomados los registros que se tratan en este cuerpo legal.[6]

Al decir "automatizado o no" hace alusión a lo que en derecho comparado es una distinción entre dos tipos de base de datos: Los **registros de datos personales automatizados,** que son aquellos organizados a partir de bases de datos, y **los registros manuales** que no utilizan en su elaboración bases de datos. Estimamos que este distingo resulta todo un acierto, en el sentido que limitar la definición al soporte automatizado

[5] Jijena Leiva, Renato, "Ley Chilena De Protección de Datos Personales. Una visión crítica desde el punto de vista de los intereses protegidos", cuadernos de extensión jurídica, Universidad de los Andes N° 5, año 2001, página 86.

[6] Mendoza Zuñiga, Ramiro Alfonso, "Régimen de los bancos de datos de organismos públicos. Una aproximación del Derecho Administrativo a la Ley Sobre Protección a la Vida Privada", cuadernos de extensión jurídica, Universidad de los Andes, N° 5, año 2001, páginas 131 a 152

habría sido lo más lógico, pero que sin duda hubiese resultado un gran error, ya que constreñir la aplicación de la ley al soporte informático y dejar sin regulación el basto campo de los soporte no informáticos habría motivado una explosión de registros manuales provocando quizá una involución tecnológica.

A nivel comparado, para hacer referencia a los sistemas de documentación informática, se utilizan las expresiones: "bancos de datos" (data bank) y "base de datos" (data base).

Para diferenciarlas se dice que las **bases de datos** se refieren a sistemas de documentación que operan con títulos o referencias. En cambio los **bancos de datos** almacenan textos o documentos.

También se ha dicho, en un afán diferenciador, que la expresión **base de datos** es propia del lenguaje técnico informático y hace referencia al conjunto de programas dirigidos a organizar la documentación, mientras que **bancos de datos** sería la expresión propia del lenguaje de las ciencias sociales y del derecho que aludirían al conjunto de informaciones pertenecientes a estos campos y que se hallarían organizadas en una o varias bases de datos.[7]

Sin embargo el hecho que en inglés la abreviatura DB sirva para hacer referencia indistintamente a Data Banks y a Data Base, ha determinado un uso indiferenciado de ambas expresiones.

Suelen distinguirse tres grandes modelos de bases o bancos de datos:

a).- Bases de datos jerárquicas (hierarchical data base), en las que los datos están organizados por relaciones de jerarquía que pueden representarse de forma arborescente a partir de una raíz común;

b).- Bases de datos reticulares (reticular data base o network data), en que las distintas informaciones se organizan a través de una pluralidad de puntos de acceso;

c).- Bases de datos relacionales (relational data bases), en la que los datos se estructuran sistemáticamente en relaciones homogéneas que permiten al usuario seleccionarlas y adaptarlas a sus necesidades operativas. Se trata de un tipo de base de datos o sistema de administración de bases de datos, que almacena la información en varias tablas (filas y columnas de datos) o ficheros independientes y realiza búsquedas que permiten relacionar

[7] Pérez Luño, Antonio – Enrique, "Ensayos sobre Informática Jurídica", Biblioteca de ética, filosofía del derecho y política, Madrid, España, Segunda Edición, año 2001, página 54.

datos que han sido almacenados en más de una tabla. El término fue acuñado en 1970 por el investigador británico Edgar F. Codd.[8]

3.- La Evolución de la Protección de Datos.

En la actualidad, los sistemas informáticos son hábiles para el tratamiento automatizado de la información, tanto textual como de imágenes y sonido, en volúmenes que hasta hace muy poco tiempo no parecían posibles. Esto ha permitido la creación de grandes *ficheros* estructurados en que se almacenan dichos documentos, los que son susceptibles de ser relacionados y consultados fácilmente a través de procedimientos específicos y que, por supuesto, es la lógica que está detrás de las bases de datos personales.

Pues bien, estos fondos documentales perfectamente pueden crearse para almacenar datos referidos a la persona y emplearse para detectar **ciertos perfiles**, a fin de tomar una determinada posición frente ésta, lo que resulta altamente peligroso por cuanto puede acarrear, como lo demuestra la experiencia histórica, discriminaciones arbitrarias respecto del titular de la información. Baste señalar como brutal ejemplo de lo anterior las tabulaciones de datos que se hicieron en la Alemania nazi, gracias a la tecnología que les proporcionaba IBM, respecto de las familias judías, su composición, relaciones parentales, y más importante aún, sus direcciones particulares.

Sin embargo, hoy en día las necesidades de información acerca de las personas recorren prácticamente todos los sectores de la sociedad, y ya se reconoce que la libre circulación de los datos personales es un imperativo no sólo para el desarrollo de la nueva economía, sino además para el funcionamiento del sistema democrático, lo que no debe hacernos olvidar los peligros que ello conlleva, sobre todo si consideramos las regresiones democráticas de los últimos años y el auge del poder de observación de las corporaciones privadas, esto deriva en que la información personal sea un bien muy codiciado por estos entes, sobre todo en lo que dice relación con compañías de seguros, empresas de colocaciones, empleadores en general y, desde luego, por el principal tenedor de datos del país: el Estado.

Especialmente preclaro ha sido al respecto Reg Whitaker, quien ha dicho:

"Los augurios respecto del control gubernamental de las bases de datos se hacen aún más sombríos con el desarrollo cada vez más importante de conexiones mediante interfaz con el sector privado, lo que conlleva diversas transferencias de datos. Ericsson y Haggerty, por ejemplo, concluyen, tras su investigación sobre la institución policial, que la cantidad de información que entra en sus bases de datos, así como la velocidad de acceso a las mismas,

[8] Edgar Frank Codd, (1923-2003), científico informático inglés conocido como el padre de la teoría de bases de datos relacionales. En la década de los años 60 y 70 trabajó en sus teorías sobre modelado de datos, publicando "A Relational Model Of Data For Shared" en 1970 (un modelo relacional de datos para grandes bancos de datos compartidos).

han transformado su naturaleza: de ser uno de los servicios más reservados del gobierno ha pasado a convertirse, gracias a las nuevas tecnologías, en un servicio de información para instituciones como las compañías de seguros, las mutuales de salud u otros servicios de asistencia social. "El interés común que comparten tanto la policía como estas organizaciones privadas consiste en la eliminación del riesgo".[9]

En la Sociedad de la Información uno de los temas fundamentales ha sido la **implementación de sistemas de identificación**, como es el caso de los controvertidos números únicos de identificación personal y otro, más controvertido aún e incluso repudiado en el mundo nórdico, son los sistemas biométricos, no obstante su promoción como "sistemas infalibles de identificación", desde el punto de vista de la técnica.[10]

El tema es de suyo complejo sobre todo si consideramos que la llamada eficiencia administrativa y las exigencias del Estado Democrático de Derecho nos llaman a perfeccionar estos sistemas de individualización, pues aunque se conciba al aparato público como un entramado de recursos materiales y humanos al servicio de la persona, no es legítimo que se llegue a establecer un sistema que en definitiva comprometa en su esencia al derecho a la autodeterminación.

Esta afirmación es consecuente con lo que dispone el artículo 29, N°s 2 y 3, y el artículo 30 de la *Declaración Universal de Derechos Humanos.*[11]

Así, la premisa que tendremos presente en este desarrollo teórico es que en nuestros días el derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la personalidad en las sociedades democráticas; sin embargo, para llegar a dicha conclusión ha tenido que pasar mucho agua bajo el puente y producirse el nacimiento, desarrollo y muerte de muchos conceptos que han influido en la evolución de la protección de datos. Por ello daremos un repaso a dichos conceptos, desde los primeros pasos o esbozos, hasta las últimas construcciones teóricas que se ha creando en las distintas épocas y lugares.

A).- Los Primeros Pasos: La "*Privacy*" Norteamérica. El derecho a la protección de datos personales ha recorrido un largo camino hasta adquirir la forma que hoy conocemos,

---

[9] Whitaker, Reg, "El Fin de la Privacidad". Editorial Paidós, Barcelona, año 1999, página 159.

[10] Se entiende por sistemas biométricos a un sistema automatizado que realiza labores de biometría, esto es, un sistema que fundamenta sus decisiones de reconocimiento mediante características reconocibles o verificables de manera automática. Una de las técnicas biométricas más maduras y confiables es el reconocimiento de huellas dactilares.

[11] Art.29 "N° 2 En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley, con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, el orden público y del bienestar general en una sociedad democrática. N°3 Estos derechos y libertades no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas."
Art. 30 "Nada en la presente Declaración podrá interpretarse en el sentido de que confiere derecho alguno al Estado, a un grupo o a una persona, para emprender y desarrollar actividades o realizar actos tendientes a la supresión de cualquiera de los derechos y libertades proclamados en esta declaración."

siendo una de las primeras fórmulas jurídicas para protegerse de los embates de la informática el buscar refugio en la antigua institución de Derecho norteamericano conocida como ***privacy***, cuyos orígenes se remontan, dijimos, a la formulación hecha por Louis Dembitz Brandeis y Samuel Dennis Warren, la cual elaboraron a partir de precedentes jurisprudenciales y publicaron como **"The Right of Privacy"**; esto es, un derecho concebido como "the right to be let alone", el "derecho a estar solo", a no ser molestado, lo que lleva aparejado como consecuencia la negación de la posibilidad de controlar la información que pertenece a la persona por el hecho de emanar o referirse a ella. Su tesis obedece a una construcción *ius privatista* de las garantías personales, que desarrolló su argumentación a partir del derecho de propiedad (*property*), específicamente de un atributo de los derechos de autor (*copyright*) como es el derecho moral al inédito, esto es a no publicar sus obras o, en este caso, actuaciones.

Pero, aunque la ***privacy*** es la fórmula que satisfizo al Derecho norteamericano para enfrentar la capacidad invasiva de las tecnologías, la realidad es que es un concepto que en origen no tiene relación alguna con la informática, si no que fue ideado en el siglo XIX como un escudo o límite a la intromisión de los periódicos y la prensa en general en la vida de las personas.[12]

B).- La recepción en el sistema continental europeo y los errores de transmisión. Como ya hemos visto, ante la irrupción del fenómeno tecnológico el sistema norteamericano echó mano de una institución jurídica antigua y flexible que le cubría los supuestos que requería proteger.

Por el contrario, los sistemas de derecho continental europeo no poseían ninguna figura semejante, con lo que se inicia una larga peregrinación en busca de la solución adecuada, siendo una de las primeras reacciones el fallido intento de "importar" el derecho a la vida privada.

Con todo, el sistema continental europeo manejaba dos conceptos fuertemente enraizados, como son la **intimidad** y la **"riservatezza"** (reserva). En su momento se vio como la solución más sencilla el equiparar **intimidad** y **reserva** con **privacidad**, la cual parecía lo suficiente elástica y amplia como para servir a este fin. Pero tanto la **intimidad** como la **reserva** tienen una naturaleza diferente: son conceptos definibles a priori y determinados, pues **intimidad** es la zona espiritual íntima (interna) de una persona y la **reserva** es "el modo de ser de la persona que consiste en la exclusión de los otros del

[12] Específicamente el artículo nace como una forma de reacción de Samuel D. Warren, famoso personaje de la vida social y política norteamericana casado con la hija de un senador, cuya vida disipada era el comidillo de los periódicos de la época.

conocimiento de cuanto se refiere a la persona misma" (tomada de Guido Alpa, *Novissimo Digesto Italiano*).[13]

Los términos intimidad y privacidad cuentan con gran similitud, pero en la teoría son diferentes. Por un lado tenemos la **intimidad,** que se refiere al espacio donde se desenvuelven las características más reservadas de la vida de un ciudadano (singularmente su domicilio- entendido como cualquier lugar donde viva, no solamente su departamento o casa, sino también una habitación de hotel o una caravana- y sus comunicaciones). Por otro lado, aparece el vocablo **privacidad**, mucho más amplio que el anterior, que agrupa a aspectos segmentados de la vida de un individuo sin significación especial, pero que agrupados, contrastados y analizados en su conjunto nos permiten obtener con detalle un perfil muy concreto de su personalidad que también ha de permanecer protegido.[14]

Lo privado tiene una definición objetiva, que se estipula en la ley; lo íntimo es siempre relativo, se refiere al círculo de personas que de manera natural tiene conocimiento de nuestra vida y nuestras decisiones; un círculo que puede ser más o menos extenso, según el caso, y carece de definición legal precisa.[15]

Según el diccionario de la RAE, por **intimidad** se debe entender una "zona espiritual íntima reservada de una persona o de un grupo, especialmente de una familia". Según la misma fuente, **privacidad** es el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Este término, aún calificado de barbarismo por parte de la doctrina (ya que proviene de la expresión inglesa privacy), no aparece en nuestro diccionario hasta 2001, así algunos opinan que no es más que un anglicismo que crea confusión en este ámbito de lo privado. Sin embargo, lo que ocurre es que, sin dejar de movernos en la esfera más íntima de una persona, nos encontramos con dos términos que presentan distintas connotaciones**.**

La **intimidad** es de estos dos conceptos el que tiene un alcance menor, pero más gravoso si se quiere. Es decir, el derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. Dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información –como la clínica o la relativa a la vida sexual- cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente. Partiendo de este punto, nacen derechos como la **inviolabilidad de las**

[13] Reusser Monsálvez, Carlos, "Privacy, Risarvatessa, Intimidad y Autodeterminación Informativa", Apuntes para la discusión. Foro Digital, año 2001, página 9.
[14] "Secreto de las comunicaciones". Microsoft ® Student 2008 [DVD] Microsoft Corporation, año 2007.
[15] Fernando Escalante Gonzalbo, "Derecho a la Privacidad", Instituto Federal de Acceso a la Información Pública, Méjico, Primera Edición, Marzo de 2004, página 23.

comunicaciones o el **derecho a la propia imagen,** ambos muy relacionados con la parte más privada de la psique del individuo.

La **privacidad,** por su parte, es un término más amplio: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por si misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo. Así, si al hablar de intimidad poníamos como ejemplos los sentimientos o creencias, podríamos ilustrar el concepto de privacidad con los libros que se consultan, las películas que se arriendan, las asociaciones a las que se pertenece, etc. Por sí solos, estos datos no tienen excesivo valor; ahora bien, tomados en conjunto, en un ambiente determinado, pueden hablarnos de los gustos del individuo, de sus preocupaciones o necesidades. En cualquier caso, sin llegar a esa zona reservada que define la intimidad. Podríamos concluir que los asuntos íntimos son privados, pero que no todos los asuntos privados son íntimos. Hecha esta distinción, es el momento en el que entra en juego el derecho a la protección de datos de carácter personal.

¿Por qué se intentó asimilar los conceptos de **privacidad, reserva** e **intimidad**? Porque los ordenamientos jurídicos continentales no tenían formas de protección de los datos de las personas frente a los sistemas automatizados de procesamiento.

C).- La "Riservatezza" Italiana. En Italia no existe un concepto equivalente al norteamericano ***privacy***, es decir, no existe una palabra italiana que abarque tal variedad y complejidad de contenidos. Así el concepto de ***privacy*** fue entusiastamente acogido en este medio, no por pura y simple convicción, si no por que cuando se descubren los peligros de la acumulación de datos para los derechos fundamentales y su falta de previsión constitucional, se ve en esta institución una efectiva herramienta para cubrir el vacío existente en la protección de datos. Y la toman literalmente, pero transformándola: entienden que ***privacy*** se refiere sólo a la protección de derechos frente a la informática y el resto de los contenidos se subsumen en los derechos fundamentales correspondientes al sistema continental europeo.

Concientes de la problemática que implica otorgarles a instituciones jurídicas nombres que no les corresponden, autores italianos, como **Mario Losano**, han abogado por la creación de términos singulares como **"privatezza",** pero con poca recepción.[16]

Doctrinariamente también se trabajó en Italia la opción de considerar que la protección de los individuos ante las bases de datos está amparada por tratarse de una de las manifestaciones de la ***riservatezza.*** Pero ya dijimos que la reserva era una forma de sustraer información del conocimiento de otros ¿entonces cómo cubrir a los datos que ya estaban fuera de ese ámbito? Pues, dicen unos, hay que ampliarla, superando sus restricciones y

[16] Reusser Monsálvez, Carlos, Op. Cit.

contemplándola desde una perspectiva abierta que llegue a entenderla como el control por parte de las personas de las informaciones que han dejado de pertenecer a su ámbito más reservado.

Lo que reconoce claramente el derecho italiano son varias formas concretas de la "reserva", como el domicilio, las comunicaciones y algunos aspectos de la libertad y del pensamiento como derechos inviolables, cuya defensa se organiza con criterios negativos, pero no existe un derecho constitucional a la ***riservatezza*** que proteja de forma global todas las facetas privadas de la persona y ello aún cuando la interpretáramos:

a).- Con un sentido amplio que cubra la protección de datos personales, y

b).- Que esta protección se pueda invocar constitucionalmente,

La **reserva** igualmente no nos serviría, por que esta institución concede una **tutela represiva y sancionatoria**, es decir, posterior a la lesión, en cambio la protección de datos lo que se busca es una tutela preventiva dirigida a evitar la posibilidad de la lesión.[17]

D).- La Vía Europea Principal: La Intimidad. En general, el derecho europeo no inicia la construcción de un sistema de protección de datos a partir de la **reserva**, si no que a partir del derecho a la **intimidad**, del derecho al **honor** y **a la propia imagen**, temas que fueron cobrando progresiva relevancia, atendido el avance del desarrollo tecnológico y su capacidad invadir diversos ámbitos de la vida.

De hecho es esta corriente la que da lugar a las primeras manifestaciones normativas de la protección de datos, ya en 1981, a través **del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal**, se reconoce expresamente la necesidad de garantizar la intimidad de las personas "teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos personales que son objeto de tratamientos automatizados" y en el plano doctrinal, en 1982, el profesor FROSINI nos evidenciaba como problemas asociados a la propia imagen en el avance de las tecnologías: "la reproducción de la imagen, interferencias telefónicas, transmisión y recepción de programas televisivos, control sobre las opiniones religiosas o políticas de los súbditos, etc."[18]

Contra lo que pueda sostenerse respecto de esta época, estimamos que ya el **Convenio 108** sienta las bases que permiten zanjar la cuestión de que las garantías fundamentales que se buscan proteger van más allá de la intimidad, al indicar en su exposición de motivos respecto de la protección de datos, que:

---

[17] Esto porque se dice que una vez producida la lesión ésta ya no puede ser reparada de ninguna forma y cualquier indemnización o reparación que se verifique se tornaría ineficaz.
[18] Frosini, Vittorio, "Cibernética, Derecho y Sociedad", Editorial Tecnos, Madrid 1982.

"El presente Convenio tiene por objeto reforzar la protección de datos, es decir, la protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal que les conciernen".

E).- El Aporte Alemán: El derecho a la Autodeterminación Informativa.

En Alemania no existe la ***privacy*** ni se la ha recogido; no existe la ***riservatezza*** y tampoco existía la ***intimidad*** en la Ley Fundamental (*Grundgesetz*) de Bonn. Pero sí se ampara la **dignidad de la persona** y **la personalidad**[19], lo que les ha permitido construir el *Recht auf informationelle Selbstbestimmung*, esto es, **el derecho a la autodeterminación informativa,** a través de una sentencia del Tribunal Constitucional Federal que declaró como violatorio de la *Grundgesetz* algunos preceptos de la Ley del Censo de 1982. Dicha sentencia reconoció que:

"En las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitada de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1 [derecho general a la personalidad propia], en relación con el artículo 1º del párrafo 1 [protección de la dignidad humana] de la ley fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona".[20]

Siendo así, independiza la **protección de datos personales** respecto de la **intimidad**, el **honor** y la **propia imagen** como garantías protegidas y recalca la función instrumental a la protección de la dignidad, la libertad y la igualdad que asisten a la persona humana en general, de las que derivan la generalidad de las garantías consagradas en los distintos catálogos de derechos.

Conforme a ello realiza una construcción a través de la cual reconoce la existencia del derecho a la **autodeterminación informativa**, que emana directamente de la dignidad de la persona que actúa con autodeterminación como miembro de una sociedad libre. Considera los peligros que entrañan para estos bienes jurídicos las condiciones imperantes en esa época y las que visualiza a futuro respecto de la elaboración automática de datos. Conforme a ello, sostiene que las necesidades de garantizar la autodeterminación demanda un nivel especial de protección, por cuanto los procesos de decisión ya no se pueden retrotraer, como antiguamente, a registros o documentos compilados manualmente. Hoy en día gracias a la ayuda de la elaboración automática de datos, la información individual

[19] Se consagra el derecho al libre desarrollo de la personalidad en tanto no lesione los derechos ajenos y no contravenga el orden constitucional o las buenas costumbres.
[20] La ley del Censo de 1982 compelía a los ciudadanos a responder más de 100 preguntas para un censo poblacional. Dada la entidad y cantidad de las interrogantes, un ciudadano se negó a responderlas, por lo que el Estado alemán accionó contra él, con las consecuencias que se traducen en la sentencia ya referida.

sobre las circunstancias personales u objetivas de una persona determinada o en su caso determinable son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquiera que sea la distancia. Es más, esa información puede -especialmente con el montaje de sistemas integrados de información- refundirse con otras colecciones de datos en un perfil de personalidad parcial o ampliamente definido, sin que el interesado pueda controlar suficientemente su exactitud y su utilización. De este modo se han ensanchado en una medida hasta ahora desconocida las posibilidades de indagación e influencia susceptibles de incidir sobre la conducta del individuo, siquiera sea por la presión psicológica que supone el interés del público en aquella.

Este derecho le **faculta para decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida,** de lo que se deduce "la libre eclosión de la personalidad del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona".[21] Como cualquier otro, se reconoce que este derecho no es absoluto, sin embargo las limitaciones que a su respecto se impongan sólo son admisibles en el marco de un interés general y necesitan un fundamento legal basado en la Constitución, que debe corresponder al imperativo de claridad normativa, inherente al Estado de Derecho. En su regulación debe el legislador observar, además, el principio de la **proporcionalidad** y tiene que adoptar asimismo precauciones de índole organizativa y de derecho a la salvaguardia de la personalidad.

Tan evidente es la vinculación de este derecho **a la libertad** y **autodeterminación del individuo** que la sentencia entiende que la conducta de la persona podrá verse afectada severamente a través de su vulneración. Así sostiene que:

"El que [la persona] no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación (...) Quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (...) esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público,

[21] Reusser Monsálvez, Carlos, Op. Cit.

porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de los ciudadanos". Continua diciendo *"De este modo, un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe bajo la elaboración automática de datos ningún "sin interés", ya que a través de ellos, sostiene, puede elaborarse "una imagen total y pormenorizada de la persona respectiva –un perfil de personalidad- incluso en el ámbito de su intimidad, convirtiéndose el ciudadano en un "hombre de cristal".*[22]

A esto último también se le conoce como la teoría del mosaico, ello porque aunque una pieza de información aisladamente considerada puede significar muy poco, al interrelacionarla con otras se va conformando un cuadro más global.

Pero ¿qué es en sí la autodeterminación informativa?

En el fondo es el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo; se trata de controlar la utilización de las informaciones personales independientemente si éstas pueden ser calificadas de íntimas, reservadas, secretas, privadas: no es relevante su mayor o menor proximidad con el ámbito o núcleo íntimo de las personas. Diversos autores han dicho a este respecto que en realidad el Tribunal Constitucional construye la **autodeterminación informativa** ante la ausencia de la consagración de la **intimidad** como derecho en la Ley Fundamental de Bonn, pero tal aproximación no es correcta, pues en realidad se trata de dos construcciones paralelas e interrelacionadas que arrancan de la personalidad y que cierran el bloque de protección de la misma.

En otras palabras: aún cuando la **intimidad** estuviera consagrada como derecho fundamental esta tampoco serviría como protección ante los embates de la informática. Entonces, hay que ir al concepto alemán de **libre personalidad**, esto es la libertad general de acción, que se concreta en la libertad para decidir la realización de determinados actos, y esta libre personalidad se expresa en la **autodeterminación informativa**, que es la libertad para determinar quién, qué y con qué motivo puede conocer datos relativos a un individuo.

Concluimos en este punto entonces que no obstante su origen primigenio, la problemática del tratamiento de datos personales progresivamente fue abstrayéndose de la sola protección de las garantías de intimidad, honor y propia imagen, fruto de la evidencia que mostró que la recogida, revelación y sistematización de información personal podía asociarse directamente con la **dignidad humana**, lo que se debe contrastar con el hecho de que las intromisiones vulneran o pueden vulnerar un cúmulo de **derechos fundamentales**, tales como la vida (como dejó en evidencia la historia reciente de muchos países afectados

[22] Reusser Monsálvez, Carlos, Op. Cit.

por dictaduras, en que los organismos del Estado recopilaban furtivamente información de los tipos de lecturas que escogían los estudiantes), la libertad sindical, el derecho al trabajo, la libertad de asociación, la seguridad personal, la intimidad, etc.

Siendo esto así, las concepciones jurídicas más avanzadas entienden hoy que **el derecho a la protección de datos integra la categoría de derecho fundamental**, y así lo consagran expresamente en su Constitución Política, directamente en el caso de Portugal, o a través de construcciones jurisprudenciales como los caso de Alemania y España, país en que su Tribunal Constitucional fue cambiando sus tesis al respecto, pasando de presentarlo como un nuevo avance, ya que hoy se le ha considerado como un derecho autónomo cuyo objetivo jurídico es proteger todos los demás derechos, fundamentales o no, reconocidos en un ordenamiento normativo.

CAPITULO II: LA PROPIEDAD DE LA INFORMACIÓN.

Un punto álgido sobre el tratamiento de datos es el tema de la propiedad de la información, más precisamente de aquella que se contiene en las bases de datos. Nuestra legislación optó por no abordarlo directamente, dejándolo al juego de las reglas generales que sobre el asunto tiene el derecho civil, produciendo con ello un enorme daño a sus titulares quienes tienen que "disputar" la propiedad de sus propios datos con las empresas que se dedican a su tratamiento. Veamos algunos aspectos:

1.- Conflicto de Intereses.

Para algunos el problema de fondo de datos es realmente un conflicto de intereses. Por un lado tenemos el interés de aquellas personas, cuyos datos nominativos se procesan electrónicamente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, filiación política, tendencias sexuales, salud, patrimonio, etc.; y por otro, un interés, también legítimo, que poseen los gobiernos y los particulares para acceder a cierta información: los Estados para cumplir con sus fines asistenciales y de orden público, como por ejemplo saber quiénes tienen SIDA al momento de fijar políticas de salud; también los particulares, generalmente constituidos en empresas de servicios o entidades gremiales quienes para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial.

La finalidad es, por tanto, lograr un equilibrio y establecer límites entre el derecho a la intimidad que consagra el artículo 19 N° 4 de la Constitución y un derecho a la información que consagra el artículo 19 N° 12, fundado en razones de orden público. La pregunta del millón en buenas cuentas es ¿son conciliables el Derecho a la Información con el Derecho a la Intimidad? No se trata la presente cuestión de un mero ejercicio teórico o doctrinal, sino de un asunto de la mayor relevancia, ya que si la respuesta es afirmativa, esto es si ambos derechos son conciliables, la pregunta que sigue es ¿cuál es ese punto de equilibrio entre la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad? En cambio si la respuesta es negativa, esto es, que ambos derechos son inconciliables de manera absoluta y total y siempre existe entre ellos una tensión que es insoluble, la labor que correspondería en tal caso sería determinar cuál de los dos derechos debería prevalecer si ambos son enfrentados en un caso concreto. Esta última situación es la que estimamos permanente y constante en el terreno práctico, esto es que ambas prerrogativas chocan permanentemente, sin que la legislación pueda armonizar de manera abstracta las posibles situaciones. Por lo tanto siempre la labor estará concentrada en determinar la primacía de uno u otro derecho en un caso concreto y dicha labor le corresponde, por atribución constitucional y legal, al Poder Judicial.

La respuesta doctrinaria a la dicotomía protección de datos – acceso a la información, ha surgido en la forma de un nuevo concepto de Derecho a la Intimidad, que surge frente a la llamada o reclamada libertad informática o de procesamiento de datos personales-nominativos, que deja de lado el enfoque individualista o negativo con que fue concebido para plantearse desde una perspectiva socializadora y positiva (ya no es "el derecho a estar solo") y que se concibe como la posibilidad de que los ciudadanos titulares y propietarios de los datos que les conciernan controlen el uso y el eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente.[23]

2.- La Propiedad de los Datos.

Como esbozamos este tema tiene gran relevancia para nuestra economía actualmente, ello debido a que varias multitiendas comerciales que exigen, al momento de otorgar créditos y facilidades de pago, una serie de datos que posteriormente almacenan de forma computacional, han vindicado pública y gremialmente la propiedad de la información. El argumento para tal afirmación es que el contenido de las bases de datos está protegido por el derecho de autor.

Alguna doctrina estima que dicho aserto es errado, toda vez que confunde "el continente" o la estructura de la base o banco de datos y "el contenido" o la información almacenada en el mismo.[24]

Las normas internacionales de mayor relevancia que aluden al tema[25] establecen que la Propiedad Intelectual ampara a las compilaciones de datos cuya selección o disposición de contenidos sean creaciones originales y señalan expresamente que dicha protección "autoral" no abarca a la información compilada o a los datos en sí mismos.

Las casas comerciales sólo pueden considerarse propietarias intelectuales del diseño y estructura original del fichero computacional, mas por el hecho de recopilar antecedentes sobre personas naturales y jurídicas, procesarlos, seleccionarlos, organizarlos o almacenarlos no se transforman en dueñas de la información nominativa que individualiza a otras personas, ello debido a que no existe título ni modo de adquirir alguno. Incluso más "el carácter de depositarias o tenedoras de datos personales les impone obligaciones de

[23] Telemática es el conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática. La telemática ofrece posibilidades de comunicación e información, tanto en el trabajo como en el hogar y otros ámbitos personales. Agrupa servicios muy diversos, por ejemplo, la telecopia, el teletexto, las redes telemáticas como Internet y las comunicaciones inalámbricas, una de cuyas aplicaciones más visibles es el Sistema de Posicionamiento Global o GPS.
[24] Jijena Leiva, Renato, Op. Cit. Página 91.
[25] Las normas internacionales de mayor importancia que aluden al tema, a saber, el acuerdo TRIP del GATT y la OMC adoptado en 1994 en Marrakech sobre los aspectos de la propiedad intelectual relacionados con el comercio (Anexo 1C, artículo 10°), la Directiva de la Unión Europea 96/9/CE de 1996 y el Tratado sobre Derecho de Autor de la OMPI adoptado a fines de 1996 en Ginebra (artículo 5°).

confidencialidad y reserva, tan importantes como aquellas que emanan del secreto estadístico o del secreto bancario".[26]

Una posición distinta es la que expresa el profesor Raúl Bertelsen que nos dice "la persona que efectúa operaciones de tratamiento datos y elabora un registro o banco de los mismos, tiene un derecho de propiedad sobre la base de datos que goza de reconocimiento y protección constitucional".

Además señala que "como resultado de la aplicación de las nuevas normas constitucionales (se refiere a la Constitución de 1980) relativas a la propiedad para adquirir el dominio de toda clase de bienes, y al derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales e incorporales, la jurisprudencia ha reconocido y otorgado protección de modo amplísimo sobre diversos y numerosos derechos de significación patrimonial. En tal sentido, y sin que la enumeración sea exhaustiva, puede recordarse cómo además de la propiedad de derechos reales –entre ellas la del derecho real de hipoteca y de servidumbres– se ha admitido la propiedad de numerosísimos derechos personales, sea que se tengan respecto de un particular o de una institución pública, sin importar tampoco que tengan su fuente en contratos particulares, en aplicación de normas legales o en disposiciones de índole administrativa. Incluso, en casos que pueden resultar audaces pero que no son sino el producto de la aplicación de las normas constitucionales a nuevas situaciones de la vida económica y social, se ha aceptado la propiedad sobre una concesión, la propiedad sobre los derechos de uso de un bien nacional de uso público, la propiedad sobre la zona de concesión otorgada a un concesionario eléctrico, la propiedad de los derechos que emanan de la calidad de estudiante, la que existe sobre el derecho a ejecutar una obra en virtud de una autorización administrativa y la propiedad sobre el derecho inmaterial de un recorrido de una línea de movilización colectiva".

El profesor Bertelsen finaliza diciendo que los ejemplos anteriormente expuestos "no son sino una demostración de la amplitud con que la Constitución Política reconoce y protege el derecho de propiedad, sin que sea necesario para reconocer la existencia de una propiedad garantizada constitucionalmente que tenga un estatuto legal propio, pues basta para ello que de la vida jurídica haya surgido una situación o una relación en que concurran las características propias del dominio".[27]

Cada uno de estos planteamientos genera problemas en relación con la información contenida en los bancos o bases de datos y en ellas en sí mismas: el derecho sobre los datos que contiene y el derecho a la base de datos como tal (recordamos la advertencia inicial

[26] Jijena Renato, Op. Cit. Página 93

[27] Bertelsen Repetto, Raúl, "Datos Personales: propiedad, libre iniciativa particular y respeto a la vida privada", cuadernos de extensión jurídica, Universidad de los Andes N° 5, año 2001, páginas 120 y 121.

sobre que en este trabajo nos concentramos en particular, en los datos personales o referidos a personas).

3.- Situación a Nivel Comparado.

Como vimos nuestra ley ha dejado en el limbo el tema de la propiedad de los datos personales, trayendo como consecuencia una serie de interpretaciones que perjudican directamente a los titulares de datos, dejándolos desprovistos de la protección legal en esa materia. En los países con arquitectura legal más elaborada se ha zanjado esta discusión utilizando algunas diferenciaciones que conviene tener presente. Tales son:

A).- Los datos personales o datos referidos/conectados a personas.

Existe una gran variedad de tipos de datos, por lo que las bases de datos contienen distintas clases de ellos: así tenemos que existen datos de carácter público, tales como direcciones, números telefónicos, etc.; también tenemos los llamados datos personales que constituyen un bien preciado para toda persona, ya que son un reflejo de su personalidad y gustos, así las creencias, afinidades políticas, ingresos, etc. Por lo anterior tenemos que existirán bases de datos que contendrán información personal como el nombre, cédula nacional de identidad, dirección, número de teléfono, correo electrónico, etc. Otras contienen información médica o historias clínicas. Otras, información general sobre las transacciones realizadas, las comidas, los bienes que se adquieren, y los movimientos de las personas, sus viajes, los viajes de su automóvil. Otras bases recopilan información sobre creencias religiosas, libros que se leen en bibliotecas, búsquedas que se realizan por Internet, tendencias políticas, sexuales, etc.

Debemos finalmente preguntarnos a quién pertenecen los datos públicos, mejor dicho, quiénes tienen derechos sobre los datos tanto privados como públicos. De esto trataremos en los siguientes puntos.

B).- La propiedad de los datos privados (datos de nombres, domicilios, teléfonos, historias clínicas, religión, etc.).

En este punto seguiremos a Ann Wells Branscomb, en su completo estudio ***¿Quién posee la información? (Who owns information ?)***[28] En relación con el nombre, dirección, y las transacciones personales Ann Wells Branscomb dice que:

"nuestros nombres, dirección y las transacciones personales es valiosa información merecedora de reconocimiento de que tenemos derechos de propiedad sobre ellos. En tanto

[28] Wells Branscomb, Ann, "Who Owns Information?, From Privacy To Public Acces", Basic Books, a division of Harper Collins Publishers, Inc., año 1994, página 29. Traducción del abogado argentino Leonardo Ghigliani, extraído de http://visitweb.com/leonardoghigliani

no reclamemos (afirmemos) estos derechos los perderemos. Si tal información tiene valor económico, tenemos que recibir algo a cambio de su uso por otros".[29]

En relación con la propiedad del número telefónico afirma:

"*El número de teléfono aisladamente considerado parecería no tener demasiada relevancia jurídica. Sin embargo, el derecho a controlar quien lo usará, cederá, transferirá es un hecho de creciente importancia. Hoy en días los números de teléfono están siendo utilizados para propósitos de identificación y se han convertido en una ventaja para la información del mercado. Actualmente comerciantes telefónicos y postales buscan obtener y usar los números para identificar los archivos de los clientes. También se trata de un medio para ubicar a los individuos. La protección de la identidad y ubicación serán asimismo asuntos de gran interés para el suscriptor individual. La manera en que los números de teléfono son emitidos, usados, protegidos y comercializados llegará en forma creciente a convertirse en uno de los puntos claves del debate público ya que los usuarios se sienten perturbados con su uso indiscriminado. Es más, las compañías deberán enfrentar mayores costos e inconvenientes para proveer tecnologías u ofrecer mayores opciones al consumidor para su protección y para revelar sus números telefónicos. El primer paso consiste en reconocer que el número de teléfono es una valiosa ventaja. Determinar el ámbito de control es el segundo paso. ¿Quién deberá tener la autoridad en este control, el proveedor del número telefónico, el usuario o el gobierno? ¿En qué casos y con qué propósitos podrá ser revelado? Y algo que es más importante, ¿Quién estará a cargo de los gastos de la imposición de ¨fixes¨ (se refiere a herramientas para reparar sofware) para diversas necesidades del usuario o del proveedor? Estas son preguntas que no pueden ser contestadas por un desencadenado mercado y tampoco por jueces o jurados carentes de sentido común en los casos que se presenten".*

Recordamos al respecto que en los EE.UU. ya se está considerando el derecho a tener un único número telefónico válido en todo el país y que se traslada con la persona.

En relación con las historias clínicas, Ann Wells Branscomb afirma que la:

"Centralización, estandarización, accesibilidad, calidad, y exactitud son todos componentes de un sistema nacional de información médica que contenga los costos y mejore la calidad de la salud. La concentración de los datos médicos también serviría para proveer un conjunto de datos para los investigadores médicos para que exista correlación entre salud y geografía, salud y hábito de dietas, salud e inoculaciones".[30]

[29] En tal sentido se ha pronunciado también la Asociación Argentina de Marketing Directo en su publicación "Marketing Directo" (carta de lectores), edición del 30/09/96.
[30] Wells Branscomb, Ann, Op.Cit.

En suma, advertimos que reivindica el derecho de las personas sobre sus datos personales de su nombre o su situación médica, como también de aquéllos otros que, si bien no son estrictamente personales como domicilio y teléfono (que quedan registrados en oficinas públicas -direcciones- o de empresas privadas) afectan íntimamente a su personalidad.

4.- La Propiedad de los Datos Públicos.

Pasamos ahora a analizar la propiedad de los datos públicos. En verdad, la cuestión no es determinar de quién son (son públicos, corresponden al Estado), sino más bien del derecho a acceder a los mismos, compartirlos, o manipularlos, comercializarlos, facilitarlos. Por ejemplo, quién puede comercializar los datos provenientes del Registro de la Propiedad Inmueble o del Registro Público de Comercio. Aquí entran en juego principios similares a los del sistema republicano de gobierno, la publicidad de los actos de gobierno.

El estudioso norteamericano, profesor Henry H. Perritt Jr.[31] sostiene que los datos originados en el ámbito federal, provincial o municipal son una importante parte de la salud republicana, siendo incompleta la infraestructura nacional de información si no se facilita el acceso a los ciudadanos.

En los EE. UU. la *Freedom Of Information Act* (FOIA) garantiza a la ciudadanía el acceso electrónico a la información. Pero como muchas oficinas gubernamentales han firmado convenios con proveedores privados de información (en particular relacionados con la información legislativa y judicial) se plantea el problema entre el referido derecho y el de los proveedores privados.

Estos últimos son preferibles al gobierno a efectos de analizar y almacenar la información y también en la forma de ponerla a disposición del público. Entonces, diversos derechos potencialmente limitan el acceso público a los registros gubernamentales, siendo el de los derechos intelectuales el más delicado. Empresas privadas han invertido mucho tiempo y dinero recolectando, mejorando, tornando accesible en suma, información pública recopilada en viejos sistemas prácticamente inaccesibles. Entonces ¿debe reconocerse su derecho a recibir una compensación de los ciudadanos por sus esfuerzos o debe primar el derecho de los ciudadanos a acceder a los registros públicos?

En síntesis, en esta materia, existe una particular tensión entre el derecho de propiedad intelectual y el acceso público a la información gubernamental.

---

[31] Seguimos en esto el trabajo del profesor Henry H. Perritt Jr. Regulation And The National Information Infraestructure § Assuring Access To Public Information (presentado en la Conference on Business and Legal aspects of the Internt and Online Services - Nueva York, 30 de Septiembre de 1994) en I. en: http://www.law.vill.edu/chron/articles/regulation_and_public_access.htm Traducción del abogado argentino Leonardo Ghigliani, extraído de http://visitweb.com/leonardoghigliani

El derecho de monopolio, que en EE. UU. garantiza la Copyright Act, choca con la meta del acceso público a la información y la política de una diversidad de fuentes y canales para el acceso a la información. (Todos estos principios y razonamientos deben ser traducidos a una realidad como la nuestra, con un mercado y una oferta de servicios mucho más limitada). Y al mismo tiempo, o como para balancear esta tensión, es cierto que considerar a todo servicio de valor agregado como afectando el derecho del público a la información puede desalentar la iniciativa privada a imaginar nuevos servicios o accesos del público a la información pública. Cómo preservar estos valores impidiendo la constitución de monopolios es uno de los mayores dilemas de la política de la información.

En conclusión el Prof. Perritt señala los principios -que compartimos- que deberían guiar los principios de la propiedad intelectual con relación a la información pública:

- La información y los valores agregados desarrollados con fondos públicos directamente por oficinas del gobierno y/o por sus contratistas, no deberían estar protegidas por el copyright,
- Cuando los servicios de valor agregado se prestan con técnicas que no pueden ser separadas de la información, todo derecho intelectual sobre las técnicas propietarias debe ser preservado, pero los contratos deberían incluir una licencia sobre los derechos de propiedad a un royalty razonable.

Para el caso chileno es un hecho cierto que es el Estado quien tiene la mayor cantidad de registros o bases de datos, ello debido a su naturaleza y finalidad. Estos datos, se dice, han sido incorrectamente conceptualizados en la Ley N° 19.628, ya que a todos ellos son agrupados bajo una nomenclatura genérica de datos de carácter personal o sencillamente datos personales, posteriormente se les define sin distinguirlos, siendo que en doctrina son tratados de forma separada, ya que, por un lado, no siempre los datos personales son datos de carácter personal, y viceversa.

En principio, los datos de carácter personal son de tres clases:

1° Datos personales en sentido estricto, que son los datos existenciales, en la medida en que puedan ser asociados a una persona identificada o identificable. Ejemplos aquí son el nacimiento, muerte, estado civil, domicilio, etc.;

2° Informaciones sobre cosas y bienes, lo que se revela en la Ley N° 19.628 con bastante amplitud al decir “cualquier información”,

3° Ejercicio de determinadas actividades.

Se trata de una enunciación no comprensiva de todos los datos, así también dentro de esta clase tenemos la información alfabética, biométrica (huellas digitales) o acústica.

Mención aparte merecen los datos que nuestra ley denomina datos sensibles, que si son propiamente datos personales, y que la ley define como *"aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y de la vida sexual".*

Desde otro punto de vista, el dato de carácter personal puede ser de dos clases: dato accesible al público y dato no accesible a público; esta diferenciación nos revela un aspecto de la actividad registral del Estado y es que dicha actividad no es, necesariamente, un camino de publicidad, de información, sino que más bien puede ser de limitación o de regulación del derecho, mas no de transparencia de la gestión administrativa.

Por lo tanto que exista un registro público no significa necesariamente que su contenido sea accesible a todas las personas, sino que la denominación es identificatoria de una situación orgánica, tenemos que *"se trata, entonces, del órgano público que contiene o mantiene ese registro para el cual el acceso de los particulares a la información contenida en ellos es regulada por las normas particulares que rijan para cada uno en particular"*.[32]

El sistema chileno actual de tratamiento de la información en cuanto a los bancos de datos en manos de organismos públicos se encuentra en la Ley N° 19.628 y en normas dispersas que se refieren, como por ej. el Estatuto Administrativo.[33] Por su parte la Ley N° 18.575, sobre Bases Generales de La Administración el Estado, presupone los principios de transparencia y publicidad de los actos de la Administración y el deber de darla a conocer a quienes la requieran a menos que concurran ciertas causales de justificación que la releven de este mandato.

Esto último se encuentra justificado por el artículo 6 de nuestra Carta Fundamental, que ordena que en todo caso la Administración está sujeta directa y expresamente a la Constitución, y por ende, le corresponde a ella (y a los funcionarios que exprese) el deber de resguardar el ámbito de intimidad de aquellos terceros que le han proveído de datos e informaciones personales. De lo expuesto surge que existen asuntos respecto de los cuales los funcionarios están en el deber de mantenerlos dentro de la esfera de intimidad que corresponde, de modo tal que si se vulnera este deber, aparte de las responsabilidades funcionarias que corresponden, el Estado está en el deber de reparar el daño que se ocasionare, por aplicación directa de los artículos 6 y 7 de la Constitución.

---

[32] Mendoza Zuñiga, Ramiro Alfonso, "Régimen de los bancos de datos de organismos públicos. Una aproximación del Derecho Administrativo a la Ley Sobre Protección a la Vida Privada", cuadernos de extensión jurídica, Universidad de los Andes, N° 5, año 2001, páginas 131 a 152.

[33] En su artículo 55, letra h) que impone como obligación a cada funcionario "guardar secreto en los asuntos que revisten el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales".

CAPÍTULO III: LA LEY NÚMERO 19.628

Es menester ahora revisar la ley que rige el tratamiento de datos personales en Chile en sus aspectos más relevantes tales como, su ámbito de aplicación, los principios en que la inspiran y los derechos que consagra.

1.- Ámbito de Aplicación.

En contrario a lo que el título sugiere, la ley no regula de manera orgánica todos los aspectos de la vida privada. Materias como la protección del domicilio, de la correspondencia, de las comunicaciones y en general, la protección del honor, la imagen y la intimidad de las personas quedaron fuera del ámbito de protección de la Ley N° 19.628 en su redacción final. Por el contrario la ley regula de manera muy específica el tratamiento de datos de carácter personal en registros o bancos de datos. Se protege la vida de las personas naturales en cuanto ésta puede verse afectada por la recolección, registro, procesamiento, comunicación o utilización que se haga de cualquier forma, manual o automatizada, de sus datos personales, en registros o bancos de datos, por parte de personas u organismos públicos o privados.

Como primera conclusión, podemos decir que se trata de una ley que, a pesar de lo ambicioso de su epígrafe, tiene un ámbito de aplicación muy limitado referido exclusivamente al tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política (art. 1°, inc. 1°, Ley N° 19.628).

Ahora, conviene saber qué es lo que nuestra legislación entiende por "tratamiento de datos". En el artículo 2° letra o) nos explica que es *"cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".*

Interesa de esta extensa definición, que más que definición pareciera una enumeración casuística de todas las posibles situaciones que se pudieran comprender, el hecho que no sólo se refiere al tratamiento de datos realizado en soporte informático, sino también en otros tipos de soporte, incluyendo claro está el soporte físico (documentos escritos, grabaciones de audio o video, etc.), el mero cruce de datos efectuados en un cuaderno se incluiría en la definición, lo cual estimamos positivo ya que el tipo de soporte en que se efectúe el tratamiento de datos es irrelevante, toda vez que lo importante es el procedimiento en sí y los efectos que de ello se derivarían.

A su turno, la letra f) del mismo artículo define a los datos de carácter personal o datos personales como *"los relativos a cualquier información concerniente a personas naturales, identificadas o identificables"*.

Esta definición no señala que clase de información estaría incluida, por el momento sólo parece estar claro que dentro del concepto de Datos Personales deben entenderse incorporados los hechos relativos a una persona que puedan ser comprobados. Ejemplos, su nombre, fecha de nacimiento, domicilio, nivel de remuneración.

La ley además crea una categoría especial de dato, denominado dato sensible, que es aquel referente a ciertos aspectos de la vida privada que serían merecedores de especial cuidado, entre los que coloca a los estados de salud físicos y psíquicos, las creencias religiosas, opiniones políticas y la vida sexual.

Importa hacer notar que el tratamiento de datos personales objeto de regulación es el que se hace en registros o bancos de datos, o sea el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos (art. 2° letra m, Ley N° 19.628). En coherencia con ello es irrelevante el soporte en que se encuentre almacenados los datos personales.

Por otro lado, la ley no distingue si el tratamiento es efectuado por sujetos de derecho público o de derecho privado y, en consecuencia, los somete básicamente a las mismas reglas.

Por último, es menester recalcar que la ley excluye de su ámbito de aplicación el tratamiento de datos personales que se efectúe en ejercicio de las libertades de opinión y de informar consagradas en el número 12, del artículo 19 de la Constitución Política del Estado, el que en definitiva debe ser regulado en la respectiva ley de quórum calificado a que se refiere el inciso primero de dicha norma constitucional, hoy en día corresponde a la Ley N° 19.733 sobre Libertades de Opinión e Información y Ejercicio del Periodismo.

Pedro Anguita Ramírez, reconoce un ámbito de protección, y señala que la Ley N° 19.628 *"protege a los titulares de datos personales respecto de los tratamientos manuales o automatizados que de ellos efectúen tanto las personas naturales o jurídicas, que sea realizado por órganos públicos o entes privados. Pretende del mismo modo tutelar los derechos fundamentales de las personas reconocidos en el ordenamiento jurídico en el ámbito de la protección de los datos de carácter personal"*.[34]

[34] Anguita Ramírez, Pedro, "La protección de datos personales y el derecho a la vida privada", Editorial Jurídica de Chile, año 2007, página 293.

2.- Principios que rigen el Tratamiento de Datos Personales en la Ley N° 19.628

A).- Se debe cumplir la ley y las finalidades permitidas en el ordenamiento jurídico.

El tratamiento de datos personales sólo puede efectuarse cuando lo autoriza el titular de los datos o la ley (art. 4°).

1).- Si es el propio titular de los datos personales quien autoriza el tratamiento de los mismos, dicha autorización debe cumplir con ciertos requisitos:

a).- La autorización debe ser escrita e informada. (art. 4°, incs. 2° y 3°) En opinión de Felipe Vial Claro *"La información que debe proporcionarse al titular de los datos debe cubrir tanto la finalidad dentro de la cual se enmarcará el tratamiento de datos como su posible comunicación al público, lo que dice relación con el grado de divulgación de sus datos personales que el titular está dispuesto a tolerar"*.[35]

b).- La autorización es revocable, también por escrito, y en ningún caso opera con efecto retroactivo.

2).- Si es la ley la que autoriza el tratamiento de datos personales, ésta puede tratarse de una ley especial (art. 4) o se encuentre genéricamente establecida en la Ley N° 19.628. Para Vial Claro la ley autoriza de forma inorgánica el tratamiento de datos en cuatro casos.

I) Si los datos personales provienen de fuentes accesibles a público, esto es no reservado a solicitantes, y siempre que se trate alternativamente de:

- datos personales de carácter económico, financiero, bancario o comercial.

- datos personales que se contengan en listados relativos a categorías de personas, que se limiten a indicar antecedentes tales como: pertenencia a un grupo, profesión o actividad, dirección, fecha de nacimiento.

- datos personales que sean necesarios para comunicaciones comerciales de respuesta directa, o comercialización o venta directa de bienes y servicios (art. 4° inc.5).

II) Si se trata de tratamiento de datos personales que efectúen personas jurídicas privadas, siempre que sean:

- datos personales para uso de la misma persona privada, sus asociados o afiliados, y

[35] Vial Claro, Felipe, "La Ley N° 19.628 Sobre Protección de Datos de Carácter Personal, Una Visión General", cuadernos de extensión jurídica, Universidad de los Andes, N° 5, año 2001, página 29.

- su tratamiento sólo sea con fines estadísticos, de tarificación u otros de beneficio general de los mismos (art.4, inc. final). La determinación de estos fines no se especifica, el ejemplo que resalta es el relativo a la investigación histórica o científica.

III) En los casos de tratamiento de datos personales que efectúen personas u organismos públicos respecto de materias de su competencia (art.20).

IV) Si el tratamiento de datos personales se efectúa para la determinación u otorgamiento de beneficios de salud que corresponda a sus titulares (art.10). Se trata aquí de un caso muy especial en que la ley autoriza el tratamiento de datos incluso sensibles, referidos a características físicas o morales de las personas, su vida privada o intimidad (entre los que se incluyen sus hábitos personales, origen racial, estados de salud físicos o psíquicos y su vida sexual). También serían sensibles aunque en otro orden de materias, las ideologías, opiniones políticas y creencias religiosas, art. 2, letra g).

B).- Se deben respetar los Derechos del Titular de los Datos.

La ley concede la condición de titular de los derechos que se reconocen al titular de los datos, únicamente a las personas naturales y no a las personas jurídicas. Esto se justifica en la convicción que el honor, la imagen y la intimidad, que esta ley protege, son atributos morales exclusivos, por su naturaleza, de las personas naturales.

Sin perjuicio de los derechos que la Constitución Política reconoce en relación con la vida privada de los individuos, la ley reconoce al titular de los datos los siguientes derechos:

1).- Consentimiento del titular de los datos para efectuar su tratamiento.

Para Vial Claro *"la ley, de alguna manera, reconoce a las personas naturales el derecho a que sus datos no sean incluidos en un registro o banco de datos personales sin previa autorización del mismo titular o de la ley"*.[36]

Este principio se concreta se asegura en el reconocimiento de las siguientes facultades:

a) Autorización previa: ya vimos que la ley impone que la autorización deba ser expresa y constar por escrito, pudiendo el titular de los datos revocarla, pero sin efecto retroactivo, lo que también debe hacerse por escrito.

b) Acceder al registro o banco de datos personales: en efecto, la ley reconoce la facultad de exigir gratuitamente, de quien se dedique al tratamiento público o privado de datos personales, información sobre los datos personales contenidos en el respectivo

[36] Vial Claro, Felipe, Op. Cit.

registro o banco de datos, su procedencia, destinatarios, la finalidad del almacenamiento y la individualización de las personas a quienes sus datos son transmitidos regularmente (art.12, inc.1°).

c) Exigir la eliminación de datos personales: la ley también reconoce la facultad de exigir gratuitamente la eliminación de datos personales, por la revocación de la autorización o por falta de fundamento legal (art. 12, inc. 3°).

2).- Sujeción del tratamiento a una finalidad.

El tratamiento de datos sólo podría efectuarse para aquellas finalidades expresamente autorizadas por el propio titular o la ley. Este derecho se asegura con el reconocimiento de algunas facultades:

a).- Utilización limitada a fines determinados: los titulares pueden exigir que los datos personales sean utilizados sólo para fines para los cuales hubieren sido recolectados (art.9).

b).- Acceder al registro o banco de datos personales (letra a) del número anterior).

c).- Exigir información al momento de recolectarse datos personales: la ley también establece que al momento de recolectar datos personales a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, se debe informar a las personas:

i) del carácter obligatorio o facultativo de las respuestas, y

ii) el propósito o finalidad para el cual se está solicitando la información (art. 3°)

d).- Facultad de oponerse a ciertos usos de los datos personales: en efecto, el titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión (art.3° inc.2°).

e).- Resguardos en la transmisión automatizada de datos: en el caso de establecerse procedimientos automatizados de transmisión, el responsable del banco de datos transmisor debe cautelar los derechos de los titulares y cuidar que la transmisión guarde relación con las tareas y finalidades de organismos participantes (art.5°, inc.1°). Igualmente, debe dejar constancia de la individualización del requirente, del motivo o propósito del requerimiento y del tipo de datos que se transmiten (art.5°, inc. 2°). Por otro lado, el receptor sólo puede utilizar los datos personales transmitidos para los fines que motivaron la transmisión (art.5°, inc.3°).

f).- Facultad de eliminar datos personales.

3).- Veracidad o Calidad de la Información.

Las personas naturales tienen derecho a que la información a su respecto contenida en los registros o bases de datos personales sea exacta, actualizada y responda con veracidad a una situación real del titular de los datos (art.9, inc. 2°). Este principio se materializa en una serie de disposiciones tendientes a hacerlo efectivo:

a).- Facultad de acceder al registro o banco de datos personales, ya vista en los numerales anteriores.

b).- Establecimiento de formas de alteración de las bases de datos personales: en este orden de cosas el titular de datos personales tiene la facultad de exigir gratuitamente la modificación, eliminación o bloqueo de sus datos personales en los siguientes casos:

1° Facultad de eliminar datos: según el art.12, la caducidad de la información autoriza a exigir la eliminación de los datos. En este caso debe procederse en general a la destrucción de los datos y, además, a dar aviso de la eliminación de un modo particular a quienes se hubiere comunicado dicha información o, de un modo general, si lo anterior no es posible, mediante un aviso que pueda ser de conocimiento general de los usuarios del respectivo banco de datos.

Le ley define como dato caduco a aquel que *"ha perdido actualidad por disposición de la ley, por el cumplimiento o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna"* (art. 2, letra d).

2° Facultad de modificar datos: la misma norma autoriza a exigir la modificación de datos erróneos, inexactos, equívocos o incompletos, caso en el cual debe procederse a cambiar el contenido de los datos almacenados y, además, a dar aviso de la modificación, en los mismos términos comentados en el párrafo anterior.

3° Facultad de bloquear datos: si no corresponde la eliminación, puede solicitarse el bloqueo cuando la exactitud de datos no puede ser establecida o si su vigencia es dudosa, caso en el cual debe procederse a la suspensión de toda forma de tratamiento (art. 12 y 6°).

Incluso más, el responsable del banco de datos debe proceder a la eliminación, modificación o bloqueo de los datos, según corresponda, sin necesidad de requerimiento del titular. Sin embargo, el derecho a exigir la eliminación, modificación o bloqueo de datos reconoce algunas excepciones, las que tienen lugar cuando el ejercicio de dichas facultades impide o entorpece el debido cumplimiento de funciones fiscalizadoras del organismo público requerido (como podría ser el caso del Servicio de Impuestos Internos), afecta la reserva o secreto establecidos en leyes y reglamentos, afecta la seguridad de la nación o el

interés nacional, o también cuando tales facultades no fueren reconocidas al titular en la ley que haya ordenado el almacenamiento de los datos (art. 15). Este derecho a exigir la eliminación, modificación o bloqueo de datos no puede ser limitado por actos o convenciones de las partes (art.13).

c).- Exactitud, actualización y veracidad de la información sobre obligaciones. Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados, por las causales que expresa el artículo 17, como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o crédito de bancos, sociedades financieras y otras instituciones que señala la misma disposición.

En ningún caso pueden comunicarse los datos anteriormente referidos que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal. Se exceptúan de estas prohibiciones a los tribunales de justicia, a los cuales se les comunicará la información que requieran, pero sólo con motivo de juicios pendientes (art. 18).

d).- Exactitud, actualización y veracidad de la información procesal y penal: cuando se trata de esta clase de información, los organismos públicos que se dedican al tratamiento de datos no podrán comunicarlos una vez prescrita la acción penal o la administrativa, o una vez cumplida o prescrita la sanción o pena (art. 21). Se exceptúan, también, los tribunales de justicia, así como "*otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto"* (art. 21).

4).- Reserva y Custodia de Datos Personales.

La ley dispone que las personas que trabajen en el tratamiento de datos personales deberán guardar reserva o secreto permanente, aun después de terminadas sus actividades en este campo, sobre los datos personales y los datos y demás antecedentes relacionados con el banco de datos (art.7).

Además, la ley obliga al responsable de la base de datos personales a cuidar dichos datos con la debida diligencia y lo hace responsable de los daños que pueda provocar al titular. Esta responsabilidad se traduce en un deber de custodia, tendiente a evitar que los datos personales sean comunicados a personas no autorizadas o que las comunicaciones sean interceptadas por personas no autorizadas (art.11).

5).- Especialidad del Tratamiento de Datos Sensibles.

Las personas naturales tienen derecho a que sus datos sensibles no sean objeto de tratamiento, sino en virtud de autorización especial al efecto dada por el titular o la ley. Dicho aserto se desprendería de lo dispuesto en el art. 10, por lo cual no sería suficiente, para legitimar el tratamiento de datos sensibles la simple autorización.

La Ley N° 19.628 define dato sensible *"aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y de la vida sexual".*

Esta disposición sigue a la normativa existente en todos los países que integran la Unión Europea, que define un conjunto de datos personales especialmente protegidos.

En principio los datos sensibles no puede ser objeto de tratamiento, sin embargo establece una serie de excepciones a dicha prohibición:

1).- Aquellos casos en que la ley lo autorice.

2).- Casos en que el titular de los datos sensibles otorgue su consentimiento.

3).- Casos en que se trate de datos personales que sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

A diferencia de la legislación europea en la cual se inspira, nuestra ley no dispuso requisitos adicionales o más exigentes para efectuar un tratamiento de datos sensibles que efectúe una persona o entidad, por lo que siguiendo la regla general del art. 4, el consentimiento del titular debe ser expreso y por escrito, al cual se le debe informar sobre el propósito del almacenamiento y su posible comunicación terceros de manera pública.[37]

Para Pedro Anguita Ramírez existe una categoría específica de dato sensible, y es la que se vincula a la salud de las personas, como se desprende de la misma definición de dato sensible del art. 2, letra g), en que habla de *"... los estados de salud físicos y psíquicos..."*. Siguiendo la regla de los datos sensibles esta clase especial de dato podrá ser objeto de tratamiento en aquellos casos en que los pacientes o enfermos lo autoricen. Se exceptúan los datos personales que sean necesarios para la determinación u otorgamiento de

[37] El poco conocimiento que los propios órganos del Estado tienen de la ley de protección de datos personales se demostró el año 2006, en tal ocasión el Ministerio de Planificación anunció la inclusión en las fichas de protección social, antes llamadas CAS, el origen racial de las personas pertenecientes a pueblos originarios, por estimarse que ello constituía un factor muy relevante en las políticas públicas destinadas a la población indígena. Sin embargo el procesamiento de dichos datos, sin el consentimiento de sus titulares, está fuera de los casos de excepción que señala la Ley N° 19.628. Fuente: El Mercurio, edición del día domingo 25 de junio de 2006, página C-7

beneficios de salud, esto por la importancia de tales antecedentes para el diagnóstico adecuado del estado de salud de los pacientes, por parte de los profesionales de la medicina. Una segunda excepción, en que no es menester que intervenga el consentimiento del paciente para efectuar el tratamiento de datos, es que éste sea necesario para salvaguardar el interés vital de sus titulares y éstos se encuentren imposibilitados de otorgar su consentimiento.

Un aspecto estrechamente vinculado a la protección de esta especial clase de datos lo constituyen las recetas y exámenes médicos. El artículo 24 de la Ley N° 19.628 añadió dos nuevos incisos al artículo 127 del Código Sanitario.

"Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo.

Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".[38]

¿Derecho a efectuar tratamientos de datos personales?

Para la doctrina la previsión establecida en el art.1°, inc. 2°, esto es que *"toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para las finalidades permitidas por el ordenamiento jurídico"*, despierta curiosidad. Se dice que no tiene parangón en el derecho comparado, ya que no hay ley de protección de datos personales en el mundo que reconozca la facultad de los ciudadanos de efectuar tratamiento de datos personales,[39] debido a que el procesamiento de datos personales es una actividad lícita, esto es, no se encuentra prohibida por lo que su mención es absolutamente innecesaria.

Se resalta lo paradójico que resulta que el primer derecho que la ley consagra no es de los titulares de datos, sino de las personas que efectúan tratamientos de datos personales, los que la ley denomina "responsables".

[38] La prensa ha puesto en evidencia a una industria que compra y vende recetas médicas, contraviniendo la ley. Fuente: El Mercurio, edición del día sábado 11 de marzo de 2006, página B-1 y 4.
[39] Anguita Ramírez, Pedro, "La protección de datos personales y el derecho a la vida privada", Editorial Jurídica de Chile, año 2007, página 305.

La ley (art. 2, inc. 2°) exige tres condiciones generales para que una persona pueda efectuar su tratamiento de datos:

1).- El tratamiento debe efectuarse de manera concordante con la Ley N° 19.628

2).- Para las finalidades permitidas por el ordenamiento jurídico.

Habíamos dicho precedentemente que dentro de los principios que inspiran nuestra legislación en materia de protección de datos se encontraba uno que se denomina "calidad de los datos", cuya manifestación es el principio de finalidad, que significa que los datos sólo pueden utilizarse para las finalidades que fueron recolectados, aunque hacen excepción a este principio los datos obtenidos de fuentes acceso público.

3).- Respetando el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la Ley N° 19.628 reconoce. Tales serían el derecho a la vida privada y a la honra de la persona, art. 19 n° 4 de la Constitución.

3.- Derechos Reconocidos Por la Ley N° 19.628

La Ley N° 19.628 consagra una serie de derechos a los titulares de datos personales entre las cuales podemos mencionar tres que resultan especialmente interesantes, habiendo aludido a los dos primeros:

1).- Derecho de acceso. Arts. 12, inciso 1°, que asegura el derecho a obtener información de manera gratuita referente a los aspectos de su vida que señala la norma. No es un derecho absoluto, ya que existen causales por las cuales se puede denegar el acceso de los datos personales:

a).- Cuando impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido. Se dice que al utilizar la expresión "organismo público", denegaría la aplicación de la causal por parte de administradores privados de bancos de datos, aunque esto es discutible.

b).- Afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional.

La ley, en los casos que proceda, le impone al responsable de la base de datos el deber de bloquearlos sin necesidad que lo requiera el titular. Art. 6°, inc. 4°.

2).- Derecho de oposición. Se consagra este derecho en un caso específico: respecto a la utilización de los datos personales con fines de publicidad, investigación de mercados o encuestas de opinión. Art. 3°, inciso 2°.

La ley dispone que sólo puede efectuarse el tratamiento de datos en los casos que el titular lo consienta expresamente o cuando dicha ley u otras disposiciones legales lo autoricen. Se consagran varias situaciones de excepción en las cuales no se requiere la voluntad del titular. Art. 4, inc. 5° y 6°. Para alguna doctrina y aunque la ley no consagra la facultad de un modo explícito, el titular puede oponerse al tratamiento de sus datos personales en los casos que la ley no disponga lo contrario.

3).- Derecho a indemnización. El titular tiene derecho a ser indemnizado por los daños patrimoniales y morales sufridos a consecuencia de un tratamiento indebido de sus datos personales. Art. 23

La Ley N° 19.628 lo consagra más que como un derecho, como un deber del responsable de la base de datos, sea éste una persona natural o jurídica, pública o privada. Es un deber compatible con la solicitud de eliminación, modificación o bloqueo de los datos personales que efectúe el titular.

El afectado por el tratamiento indebido de sus datos personales tiene tres caminos:

1°.- Deducir únicamente la acción de indemnización de perjuicios, sin que el titular de los datos personales ejerza la acción de reclamación, la cual se rige por el procedimiento sumario.

2°.- Ejercer la acción de indemnización de perjuicios junto a la acción de reclamación, que persigue establecer una infracción a la ley, lo cual es compatible con la solicitud de eliminación, modificación o bloqueo de sus datos. El ejercicio de la acción de resarcimiento se rige también por el procedimiento sumario, al igual que las infracciones no contempladas en los artículos 16 y 19 de la Ley N° 19.628.

3°.- Deducir una demanda de indemnización de perjuicios, la cual se sujetará a las normas de responsabilidad extra contractual, del Libro IV del Código Civil, de acuerdo al procedimiento ordinario contemplado en el Código de Procedimiento Civil.

Las acciones de indemnización de perjuicios y de reclamación por infracción se rigen por la normas del procedimiento sumario.

El juez podrá tomar todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que la ley consagra. El juez apreciará la prueba en conciencia. El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

4.- La autoridad de control: El Consejo para la Transparencia.

La Ley N° 19.628 no contempló un organismo administrativo, agencia, comisión o superintendencia estatal, encargado de la fiscalización y aplicación de las disposiciones del régimen jurídico de los datos personales. Esto es considerado por la doctrina como uno de puntos más débiles de nuestra legislación sobre protección de datos personales.[40]

La única referencia que se hizo al tema fue encomendar al Servicio de Registro Civil e Identificación el deber de llevar un registro de las bases de datos a cargo de los organismos públicos. La ley se remite al reglamento para la determinación de las condiciones y particularidades del registro.[41]

Fue preciso esperar hasta la dictación de la Ley N° 20.285, publicada en el Diario Oficial el 20 de Agosto del año 2008, para subsanar esa omisión. Dicha normativa denominada "Sobre Acceso a la Información Pública", que comenzó a regir ocho meses después de su publicación (el 20 de Abril de 2009), crea en su título V un nuevo organismo denominado CONSEJO PARA LA TRANSPARENCIA (en adelante CPT) Las funciones de este ente se especifican en los artículos 32 y 33 de la ley, sobre todo en este último, el cual señala un listado de funciones y atribuciones con las cuales se le dota para su funcionamiento. Precisamente es el artículo 33 en su letra m) el que nos atañe en lo relativo a la Ley N° 19.628, cuyo texto señala:

"Artículo 33 El Consejo (para la Transparencia) tendrá las siguientes funciones y atribuciones:

m) Velar por el adecuado cumplimiento de la Ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado".

La dictación de la Ley Nº 20.285, sobre acceso a la información pública, viene a desarrollar el principio de publicidad contenido en el inc. 2º del art. 8º de la Constitución reformado por la Ley Nº 20.050.- (2005).

No es este el lugar para comentar en detalle esta nueva ley, sin embargo mencionaremos algunos aspectos considerados especialmente interesantes por doctrina:[42]

La clave de bóveda de la Ley de Acceso a la Información Pública es la creación del ya mencionado CPT. Este organismo queda encargado de fiscalizar el cumplimiento de las

---

[40] Magliona Markovicth, Claudio, en "Chile: Protección de Datos Personales Políticos de Privacidad", publicado en Alfa-Redi, Revista de Derecho Informático, N° 101, Febrero, 2002.
Anguita Ramírez, Pedro, "La protección de datos personales y el derecho a la vida privada", Editorial Jurídica de Chile, año 2007, página 322.

[41] Artículo 22 de la Ley N° 19.628.

[42] Rajevic Mosler, Enrique "Una vuelta de tuerca en materia de acceso a la información", año 2008, publicado en www.fundaciónproacceso.cl

normas sobre transparencia activa y resolver los reclamos en contra de las negativas a las solicitudes de acceso a la información, además de velar porque la Administración Pública cumpla la Ley Nº 19.628, de protección de datos personales (esto último siguiendo el modelo del "Information Commissioner", del Reino Unido, en una línea que podría profundizarse). Su configuración es curiosa: una "corporación autónoma de derecho público" (art. 31), que propondrá al Presidente sus propios "estatutos" (art. 41) y cuyos empleados se sujetan al Código del Trabajo (art. 43), Su dirección y administración superior corresponde a un Consejo Directivo integrado por 4 consejeros –contra la tendencia general de órganos colegiados impares, evitando empates- designados por el Presidente de la República "previo acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio" (art. 36). La proposición debe formularse en un solo acto y el Senado debe pronunciarse respecto de la propuesta como una unidad (la primera designación debe hacerse 60 días tras la publicación de la ley). Su duración es de 6 años, la presidencia –con voto dirimente- rotativa (cada uno 18 meses) y sólo cabe la remoción acordada por la Corte Suprema, ante razones calificadas y a petición de otras autoridades (art. 38). La alta mayoría requerida para el nombramiento exigirá que en su integración no haya sólo representantes de la fuerza gobernante, y las garantías contra su remoción arbitraria garantizan el llamado "deber de ingratitud". Este sistema se asemeja al del Consejo Nacional de Televisión, el directorio de Televisión Nacional de Chile y, más recientemente, el Consejo de Alta Dirección Pública, pero a diferencia de aquéllos no existe un integrante designado por el Presidente de la República, lo que lo transforma en una entidad todavía más autónoma.

La naturaleza jurídica del CPT que hemos examinado puede calificarse sin dificultad de *sui generis* y deriva de su especial función: fiscalizar a otros organismos públicos, obligarlos a entregar información e, incluso, sancionar directamente a los infractores de la ley (Título VI). Aunque su credibilidad hacía indispensable concederle una alta dosis de autonomía no podía llegarse a una especie de islote autárquico dentro de nuestra institucionalidad pública, como en algún momento se planteó. La Constitución establece que el ejercicio de la soberanía "se realiza por el pueblo a través del plebiscito y de elecciones periódicas y, también, por las autoridades que esta Constitución establece" (art. 5º), como el Gobierno, la Administración, el Congreso Nacional, el Poder Judicial, etc. El CPT no podía estar en un limbo; debía adscribirse a una de ellas (así lo plantearon, entre otros, el Contralor Ramiro Mendoza y el profesor Jorge Bermúdez). De las disposiciones de la Ley se desprende implícitamente que el Consejo para la Transparencia integra la Administración del Estado, como una entidad autónoma de las señaladas en el art. 65, inc. 4º Nº 2 y Nº 3, de la Constitución. En efecto, el art. 31 dispone que los D.S. referidos al Consejo que no se vinculen con un Ministerio determinado "serán expedidos a través del Ministerio Secretaría General de la Presidencia" y el art. 43 excluye al CPT de una serie de disposiciones típicas de la Administración del Estado –como la toma de razón de sus

resoluciones- aplicándole otras. De allí que en la sentencia del Tribunal Constitucional 1051/2008 los Ministros Navarro y Venegas estimen "constitucionalmente desaconsejable" que "potestades jurisdiccionales" -como serían, a juicio de ambos, las asignadas al CPT- se entreguen a un órgano integrante de la Administración del Estado, que precisamente "juzgaría" a aquélla.

5.- Reglamento de la Ley N°19.628

El artículo 22, inc. 1°, de la ley señala *"El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos"*. El registro señalado tendrá un carácter público y en él deberá constar respecto de cada uno de los bancos los aspectos que señala, esto es:

- El fundamento jurídico de su existencia.
- Su finalidad.
- Tipos de datos almacenados.
- Descripción del universo de personas que comprende.

Todos estos aspectos serán definidos en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.

El reglamento señalado lo dictó el Ministerio de Justicia mediante Decreto N° 779, publicado en el Diario Oficial el 11 de noviembre del año 2000, el cual dispuso a su vez que el procedimiento de inscripción de los bancos de datos personales debía fijarse mediante resolución del Director Nacional del Servicio de Registro Civil e Identificación.

El reglamento dispone que el Registro Civil llevará el registro de los bancos de datos personales a cargo de organismos públicos, en el cual se inscribirán todos los bancos de datos personales que de acuerdo con la ley respectiva lleven las autoridades, órganos del Estado regulados por la Constitución, y los comprendidos en el inciso segundo del art. 1° de la Ley N° 18.575, orgánica constitucional de bases generales de la administración del Estado.[43]

[43] Art.1°, inc. 2° Ley N° 18.575 "La administración del Estado estará constituida por los Ministerios, Superintendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley."

CAPÍTULO IV: LA PROTECCIÓN DE DATOS PERSONALES.

La Ley N° 19.628 exigió escasas medidas de seguridad a los responsables del tratamiento de datos personales, siendo una de las falencias más destacadas que no se dispuso de un deber general, sino sólo la obligación de cuidar de los datos. Esto se traduce en que se impone a los responsables de los registros o bases de datos donde se almacenen datos personales con posterioridad a su recolección, la obligación de cuidarlos con la debida diligencia, asignándole la responsabilidad por los daños que se causen.

1.- Procedimiento de Amparo: El Habeas Data.

Como señalamos, la Ley N° 19.628 confiere al titular de datos personales un conjunto de derechos, tales como el derecho de acceso, modificación, cancelación o bloqueo. Para ejercer estas facultades el titular de datos personales debe hacer la solicitud pertinente al responsable de la base de datos, y si éste no se pronunciare dentro de dos días hábiles, o la denegare por causa distintas a la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, solicitando amparo a los derechos señalados precedentemente.

En el derecho comparado la acción conferida a los titulares de datos personales suele denominarse "acción de habeas data". En el art.16 de nuestra ley se utiliza la expresión "amparo" y en el art.17 se emplea el término "reclamación".

El profesor Pedro Anguita estima que aunque la ley no lo señala expresamente se puede inferir que *"sólo los organismos públicos pueden invocar la causal seguridad de la nación o interés nacional para denegar el acceso, modificación o bloqueo requerido por el titular de datos personales"*.

Para solventar su posición da dos argumentos: Primero, dice que difícilmente una base de datos en poder de privados puede poseer antecedentes que puedan afectar a los titulares. Segundo: el artículo 16, inciso 3°, ordena a la sala de la Corte Suprema, luego de presentado el reclamo, solicitar un informe *"a la autoridad de que se trate por la vía que considere más rápida"*.[44]

Estimamos que el primero de los argumentos esgrimidos es bastante feble, ya que, si bien es cierto lo más común es que sean los organismos públicos quienes mantengan bases de datos que sean sensibles para la seguridad de la nación o el interés nacional, también organizaciones o empresas privadas y aún particulares pueden manejar tales antecedentes para fines lícitos y de su competencia, ej. contratistas militares, centros de estudio o pensamiento (los llamados *think tank*), analistas de inteligencia independientes que realizan trabajos para publicaciones nacionales o internacionales, publicaciones del área de la

[44] Anguita Ramírez, Pedro, Op. Cit.

defensa, etc., por lo que no sería lógico que no pudieran esgrimir estas causales, a fin de proteger información sensible que pudieren tener para la seguridad de la nación o los intereses nacionales.

Sobre lo dicho al final conviene aclarar algunas expresiones, al decir "seguridad de la nación" se alude a información que pueda poner en peligro nuestra integridad territorial o nuestra existencia como nación, entre estos tenemos información sobre el número y ubicación de efectivos militares, contenido de alianzas estratégicas y similares. La expresión "interés de la nación" dice relación con antecedentes que sean valiosos para el desarrollo de nuestro aparato productivo y el bienestar tanto moral como material de la población en general, ejemplos serían datos sobre la ubicación de recursos naturales, sistema impositivo, tratados de libre comercio, etc.

En cuanto al argumento de texto señalado, art. 16, inc. 3°, no creemos que por esa sola mención se esté impidiendo a entes privados invocar las causales señaladas, toda vez que el artículo señala que se requerirá informe a la autoridad *de que se trate*, mas no a la autoridad recurrida, por lo que podría darse el caso que se solicite informe a una autoridad que diga relación con la materia en cuestión (por ejemplo la Superintendencia de Isapre o A.F.P.), pero que no sea responsable directo de la base de datos personales (como la Isapre o A.F.P.). En tal caso no podríamos considerar que las entidades privadas estén necesaria e inevitablemente excluidas de invocar las causales señaladas.

En lo referente al procedimiento de amparo propiamente tal, tenemos que la Ley N° 19.628 dispuso de dos caminos a seguir según cual sea la causal que invoque el responsable de la base de datos para denegar la solicitud: procedimiento de amparo ordinario y procedimiento de amparo especial.

A).- Procedimiento de Amparo ordinario.

1).- Causales para denegar la solicitud de información, modificación, cancelación o bloqueo de datos personales:

a).- Impedir o entorpecer el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido.

b).- Afectar la reserva o secreto establecido en disposiciones legales o reglamentarias.

c).- Tratarse de datos personales almacenados por mandato legal, de los cuales no puede solicitarse la modificación, cancelación o bloqueo, fuera de los casos que contempla la respectiva ley.

2).- Tribunal competente:

a).- En primera instancia es el Juzgado de Letras en lo Civil que corresponda al domicilio del responsable de la base de datos, que se encuentre de turno, según las reglas generales sobre distribución de causas.

b).- En segunda instancia es la Corte de Apelaciones respectiva, la cual conoce en sala.

3).- Procedimiento judicial:

Éste se rige por las reglas expresadas en el artículo 16, inciso 2°, letras a) a la h), las cuales ordenan, entre otras cosas, señalar claramente la infracción cometida, los hechos que la configuran y acompañar los medios de prueba que puedan acreditarlos. La notificación se hará por cédula, en el domicilio del responsable de datos, el cual debe presentar sus descargos dentro del quinto día, adjuntando sus medios de prueba. El juez apreciará la prueba en conciencia.

B).- Procedimiento de Amparo especial.

1).- Las causales son:

a).- Seguridad de la Nación.

b).- Interés nacional.

2).- El tribunal competente en única instancia es la Corte Suprema, que conoce en sala.

3).- En cuanto al procedimiento judicial tenemos:

a).- Interpuesta la reclamación debido a una denegación del requirente por las causales señaladas, el tribunal solicitará informe a la autoridad respectiva por la vía que considere más rápida, fijándole un plazo.

b).- La causa se conoce en cuenta. No obstante si la Corte lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación, agregándose de manera extraordinaria a la tabla.

c).- En caso de rendirse prueba, ésta deberá consignarse en un cuaderno separado y reservado, el cual conservará dicho carácter incluso una vez afinada la causa. El tribunal apreciará la prueba rendida en conciencia.

d).- En caso de acogerse la reclamación, el tribunal deberá fijar en la misma sentencia un plazo prudencial para que se dé cumplimiento a lo resuelto pudiendo aplicar una multa de una a diez unidades tributarias mensuales. Y si el responsable del banco de datos no entrega en forma oportuna o retarda la modificación ordenada por el tribunal, será castigado con multa de dos a cincuenta unidades tributarias mensuales.

e).- Si el responsable de la base de datos fuese un organismo público, el tribunal podrá sancionar al jefe del servicio con la suspensión de su cargo por un lapso de cinco a quince días.

2.- ¿Habeas Data o Habeas Dato?

Como dijimos, la nomenclatura más difundida a nivel comparado para designar a la acción que tutela y resguarda los datos personales contenidos en bases o bancos de datos es la de habeas data, sin embargo y contra esta tendencia, nuestro legislador evitó usar dicha expresión, quizá motivado por el hecho que esta acción no se encuentra consagrada a nivel constitucional, sino simplemente legal, lo cual conspiraría para equipararla al antiguo y conocido habeas corpus.

En todo caso la doctrina hace manifiesto su deseo de que tal consagración en la Carta Fundamental se verifique a la brevedad posible. Por lo expuesto conviene analizar este importante estatuto jurídico.

La locución de origen latino Habeas Data, caracteriza la institución destinada a garantizar el derecho de los individuos, los grupos y las instituciones de decidir por sí mismos cuando, cómo y en que medida pueden ser transmitidas a terceros informaciones que los atañen directamente. Etimológicamente, Hábeas, segunda persona del subjuntivo de **"habeo, habere...",** significa "**tengas en su posesión"**, que es una de las acepciones del verbo; y Data, acusativo plural de "datum", es definido por los diccionarios más modernos como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos.

Muy por el contrario, el diccionario de la Real Academia de la Lengua Española define el vocablo data, como la "nota o indicación del lugar y tiempo en que se hace o sucede una cosa, y especialmente la que se pone al principio o al final de una carta o cualquier otro documento".[45] [46]

Se puede decir que en castellano la denominación de habeas data no expresa a cabalidad la esencia de la institución. De ahí que la expresión más acertada hubiese sido habeas dato, entendiéndose doctrinariamente de la siguiente manera: traedme el dato para ordenar su exhibición o rectificación.

Para resumir y como nos señala el profesor Humberto Nogueira "la expresión habeas data significa que *<tengas los datos>* y su objeto es asegurar el acceso a la información que de la persona afectada tengan registros o bancos de datos públicos o privados, con el objeto de proteger la vida privada, intimidad, buena reputación u honra de las personas".[47]

El habeas data, en cuanto a su naturaleza jurídica, constituye una acción jurisdiccional protectora de la libertad informática o derecho de autodeterminación informativa (conocimiento y control de datos referidos a personas) y protección de la vida privada, imagen, honra o reputación de la persona, frente a la recolección, transmisión y

[45] Diccionario de la Real Academia de la Lengua Española, Microsoft ® Encarta © 1993-2007, Microsoft Corporation.
[46] Del lat. tardío (charta) data, propiamente 'documento dado', es decir, extendido, otorgado, palabra que en las escrituras latinas precede a la indicación del lugar y la fecha. Microsoft® Encarta® 2008. © 1993-2007 Microsoft Corporation. Reservados todos los derechos.
[47] Nogueira Alcalá, Humberto "Autodeterminación Informativa y Habeas Data en Chile e Información Comparativa", biblioteca jurídica virtual del instituto de investigaciones jurídicas de la Universidad Nacional Autónoma de Méjico, página 458 (www.juridicas.unam.mx)

publicidad de información que forma parte de la vida privada o intimidad de la persona desarrollada por registros o bancos de datos públicos o privados.[48]

Por su parte Pérez Luño señala "el habeas data constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, la que en la primera generación correspondió al habeas corpus respecto de la libertad física o de movimiento de las personas".[49]

En diversos países de América del Sur, como por ejemplo Argentina, Bolivia, Colombia, Paraguay, Perú y Venezuela, esta acción jurisdiccional forma parte de las acciones constitucionales protectoras de derechos fundamentales. En algunos casos tal acción opera con un procedimiento autónomo y en otras oportunidades opera a través de la acción de amparo o tutela de derechos fundamentales.

3.- Sujeto Activo y Sujeto Pasivo del Habeas Data.

El **sujeto activo** del habeas data en el ámbito sudamericano es toda persona, nacional o extranjera, la que puede actuar personalmente o representada

Los **sujetos pasivos** son los responsables de los bancos de datos ya sean entidades tanto públicas como privadas. En algunos casos, como los de Brasil y Paraguay, se limita el habeas data de manera poco aconsejable solo a entidades gubernamentales o de carácter público, dejando a las personas sin protección frente a los archivos y bancos de datos privados.

Debe señalarse que se excluyen como sujetos pasivos de habeas data los registros privados de carácter personal que no estén destinados a proveer informes a terceros, ya que se encuentran protegidos por el derecho a la inviolabilidad de los documentos privados, protegido constitucionalmente.

Asimismo hay que destacar en los respectivos ordenamientos jurídicos la exclusión del habeas data en materia de archivos y fuentes de información periodísticas, como lo hacen las constituciones de Bolivia y Venezuela, con redacciones diferentes.[50]

4.- Clases de Habeas Data: Podemos decir que se clasifican.

a).- Propios (ejercidos en estricta conexión con el tratamiento de datos de carácter personal) e **impropios** (utilizados para resolver problemáticas conexas, pero diferenciables, como el acceso a la información pública o el derecho de réplica).

---

[48] Nogueira Alcalá, Humberto, Op. Cit.
[49] Pérez Luño, Antonio – Enrique, "Del Habeas Corpus al Habeas Data", Madrid, Aranzi, 1991, página 174.
[50] Nogueira Alcalá, Humberto, Op. Cit., página 459.

b).- Individuales y Colectivos (según si es ejercido a título personal o en representación de un número determinado o indeterminado de personas).

c).- Preventivos (persiguen evitar daños no consumados) y **Reparadores** (cuyo objetivo es el de subsanar daños ya proferidos o que se están ocasionando).

5.- Características de nuestro Habeas Data.

Para efectos de sistematización trataremos de encuadrar nuestro Habeas Data a la luz de las diversas especies, subespecies, tipos y subtipos de hábeas data vigentes en el derecho latinoamericano, siguiendo troncalmente la propuesta clasificatoria de SAGÜÉS.[51]

En primer lugar debemos decir que se trata no propiamente de un Habeas Data, ya que, para ser tal, es necesaria la consagración constitucional y no a nivel simplemente legal, como lo está en nuestro ordenamiento jurídico.

En segundo lugar y siguiendo a SAGÜÉS, podemos decir que se trata de un Habeas Data de carácter **propio**, de tipo **informativo**, con lo cual queremos decir que no está destinado a operar sobre los datos registrados, sino que solamente procura recabar la información necesaria para permitir a su promotor decidir a partir de ésta, si es que la información no la obtuvo antes por vía extrajudicial, si los datos y el sistema de información está funcionando legalmente o si, por el contrario no lo está y por lo tanto solicitará operaciones sobre los asientos registrados o sobre el sistema de información en sí mismo. Esta característica se aprecia con toda claridad en los artículos 9, al manifestar que *"los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público"* y en el art.12 al decir que *"toda persona tiene derecho a exigir a quien sea responsable de un banco ...información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos".*

En tercer lugar se puede decir que estamos frente a un Habeas Data de subtipo **inclusorio**, puesto que su finalidad es la de operar sobre un registro que ha omitido asentar los datos del interesado, quien se encuentra perjudicado por dicha omisión (V.gr., el titular de un establecimiento hotelero cuyo dato no figura en un banco de datos del Servicio Nacional de Turismo destinada a los turistas en los aeropuertos) Este elemento resalta en el artículos 6 inciso 2°, al expresar que los datos personales *"han de ser modificados cuando sean erróneos, inexactos, equívocos o* ***incompletos****"* y también en el artículo 9 de la Ley.

[51] Sagüés, Néstor Pedro, "Derecho Procesal Constitucional", Tomo III, "Acción de Amparo", Buenos Aires, 1993.

Una cuarta característica de nuestro Habeas Data es ser **rectificador o correctivo**, lo cual significa que está dirigido a corregir no sólo a los datos falsos (aquellos que no se corresponden en lo más mínimo con la realidad), sino también a los inexactos o imprecisos (V.gr., el dato registrado es incompleto o puede dar lugar a más de una interpretación). Este aspecto también se pone de relieve en el art. 6 inc. 2° de la ley.

Un quinto rasgo distintivo es su carácter **exclutorio o cancelatorio**, con que se quiere decir que está diseñado para eliminar total o parcialmente los datos almacenados respecto de determinada persona, cuando por algún motivo no deben mantenerse incluidos en el sistema de información de que se trate. Es el inciso 1° del artículo 6 el que evidencia esta característica de manera más palmaria al expresar que *"los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal"*.

CAPÍTULO IV: CONCLUSIONES FINALES.

No existe en Chile un amplio desarrollo de la doctrina en el ámbito de la protección de datos personales, siendo pocos los autores que han estudiado el iter legislativo que concluyó con la dictación de la Ley Sobre Protección De La Vida Privada y De Los Datos De Carácter Personal.

Uno de esos estudiosos es el profesor Renato Jijena, quien ha dicho *"...que la protección legal de datos personales constituye un tópico jurídico con bastante perspectiva en países extranjeros, pero que en nuestro país constituye una realidad desconocida y poco estudiada"*.[52]

Sobre la Ley N° 19.628 este autor señala drásticamente que *"fue redactada a instancias de la asesoría de los grupos y empresas interesadas en asegurar el lucrativo negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento inexcusable de los parlamentarios, que siguen jactándose de su autoría con fines de marketing"*.[53]

Las empresas y grupos aludidos son Dicom S.A., filial de la transnacional estadounidense Equifax, Asociación de Marketing Directo, Cámara de Comercio de Santiago y Cámara Nacional de Comercio de Chile.[54]

En oposición a lo expuesto Claudio Magliona, ha sostenido *"que la Ley N° 19.628 significó un progreso para el derecho informático nacional y para la protección de los derechos de las personas frente al tratamiento abusivo de sus datos personales, aunque sugirió introducir cambios a la ley, algunos de los cuales ya habían sido propuestos por Jijena Leiva"*.[55]

No pretendemos negar que la publicación de la Ley N° 19.628 representó un avance con respecto a la situación anteriormente existente, sin embargo concordamos con la opinión esbozada por el profesor Jijena, en orden a señalar que la normativa pretendió favorecer principalmente a los incumbentes, esto a las empresas mencionadas y cuyo interés primordial es seguir comercializando los antecedentes personales de millones de chilenos. Sin embargo también coincidimos en que como legislación representa un aporte que tiene la enorme ventaja en que es perfectible y el momento de efectuar tal perfeccionamiento ya ha llegado.

---

[52] Jijena Leiva, Renato, "Comercio Electrónico, Firma Digital y Derecho", Análisis de la Ley N° 19.799, Editorial Jurídica de Chile, Santiago, Chile, página 76.
[53] Jijena Leiva, Renato, Op. Cit., página 77.
[54] Jijena Leiva, Renato, Op. Cit., página 77.
[55] Citado por Anguita, Pedro en "La protección de datos personales y el derecho a la vida privada", Editorial Jurídica de Chile, Santiago, Chile, página 332.

Consideramos que los puntos a corregir vienen dados, en primer lugar, por la creación de un registro público de bases de datos privadas[56]. Resulta incompresible que no se tenga noción de quiénes son las empresas o particulares que disponen de datos personales, ello resulta ilógico y consideramos que es un área oscura en la que conviene hacer luz a la brevedad.

Por otro lado creemos firmemente que debe implementar la obligación legal de informar previamente por parte del responsable de una base de datos al titular de los mismos respecto de los cuales se pretende efectuar un tratamiento[57]. Ello da garantías de transparencia y, por lo demás, al hacer sabedor al titular de la circunstancia que sus datos serán objeto de tratamiento lo pondrá en alerta para efectuar el debido seguimiento a fin que esa información no sea utilizada en su propio perjuicio.

Estimamos en tercer lugar que se requieren normas más precisas sobre la cesión de datos personales.[58] Esto a fin de darle mayor regulación a un tema de alta trascendencia por el impacto que tiene en las transacciones de un bien tan preciado.

Unido a lo anterior creemos que se debiera aclarar un punto que según hemos visto nuestra ley no abordó y que ha traído problemas en la práctica, se trata del tema de la propiedad de los datos. Como vimos, al estar regulado de manera explícita se evitaría la situación actual, esto es que se esbocen las más diversas interpretaciones por parte de las empresas tenedoras de datos a fin de demostrar que éstos son de su propiedad. Esta interpretación la estimamos de suyo perjudicial para los titulares de datos, toda vez que le da a los datos personales la calidad de bienes mostrencos, esto es susceptible de apropiación por parte de cualquiera.

Otro aspecto que estimamos digno de ser considerado es que a juicio de la doctrina se impone la necesidad de ampliar los casos en que el titular pueda oponerse a un procesamiento de sus datos.[59] Este falencia da otro argumento para solventar la tesis que la ley de protección a la vida privada no se inspiró en la idea primordial que da a entender su epígrafe (proteger la vida privada), si no más bien se pretendió asegurar el lucrativo negocio de tratamiento de datos de carácter personal para quienes se dedican a él.

La doctrina también apunta a que se deben estudiar las facultades del Servicio de Registro Civil e Identificación respecto al registro de las bases de datos de los organismos públicos.[60]

---

[56] Magliona, Claudio, "Chile: Protección de Datos Personales. Políticas de Privacidad", publicado en Alfa-Redi, Revista de Derecho Informático, N° 101, Febrero 2002, http://www.alfa-redi.org/revista/data/45-3.asp
[57] Magliona, Claudio, Op. Cit.
[58] Magliona, Claudio, Op. Cit.
[59] Magliona, Claudio, Op. Cit.
[60] Magliona, Claudio, Op. Cit.

También se debe limitar la capacidad del Estado y sus organismos de excepcionarse del cumplimiento de la ley a casos específicos y restringidos.[61] Estimamos que es conveniente reforzar la idea que el principal tenedor de datos personales del país, esto es, el Estado de Chile, no debe actuar en esta materia con un estándar más bajo que el que se le exige a los privados. Una de las finalidades del Estado es promover el bien común por lo que es inadmisible que el no cumplimiento de una disposición legal sea admitido de manera amplia, sino sólo a casos puntuales justificados por situaciones de excepción.

Un punto sobre el cual la doctrina también ha hecho hincapié es la falta de información adecuada y suficiente como para crear conciencia sobre el tema de protección de datos personales.[62] Este no es un tema menor toda vez que creemos que parte importante de la políticas de protección de los llamados derechos de tercera generación es crear en la población la idea fuerza que nos estamos frente a meras aspiraciones con cero obligatoriedad de cumplimiento, sino a derechos absolutamente exigibles. Mientras más informados estemos los ciudadanos de cuáles son nuestros derechos y de los mecanismos para efectuar esa protección, la mitad de la tarea ya estará hecha. No se puede valorar y proteger aquello que se desconoce.

Alguna doctrina estima que la Ley N° 19.628, al precisar el sentido y alcance de una garantía constitucional contenida en la Carta Fundamental efectúa una actividad interpretativa, razón por la cual el legislador no pudo regular dicha materia mediante una ley ordinaria aprobada sin el quórum exigido por la Constitución.[63] No compartimos esta opinión toda vez que, como dijimos al comienzo de este trabajo, más que regular la vida privada en su totalidad, la ley se circunscribió a un ámbito específico, cual es la protección de datos personales. Estimamos que no estamos frente a un texto que interprete un precepto constitucional, sino más bien, a un texto que desarrolla una garantía asegurada por nuestro Código Político y lo hace en uno de sus posibles aspectos solamente.

Incluso se ha dicho que, después de atribuir a la Ley N° 19.628 el carácter de ley de protección de datos de tercera generación, que estas leyes deben flexibilizar los requerimientos de protección de la privacidad de las personas, con la libertad de empresa y de información.[64] Estamos contestes en que estos dos últimos ámbitos deben ser asegurados a los particulares para prosperidad de la Nación toda, sin embargo no creemos que dicha flexibilización deba amparar una situación que estimamos perniciosa, cual es que en aras del libre emprendimiento se pretenda hacer caso omiso de la adecuada protección a una

[61] Magliona, Claudio, Op. Cit.
[62] Herrera Bravo, Rodolfo, "La protección de datos personales como garantía básica de los derechos fundamentales", Revista de Derecho Público de la Agrupación de Abogados de la Contraloría General de la República, año 2, n°5, Mayo/Agosto, 2001, página 83.
[63] Vásquez Márquez, José Ignacio, "Análisis crítico sobre la naturaleza jurídica de la ley de protección a la vida privada", Revista de Derecho de la universidad Finis Térrae, año III, N°3, año 1999, página 48
[64] Corral Talciani, Hernán, "El derecho a la privacidad y los sistemas de tratamiento de datos personales en la Ley N° 19.628, Revista de Derecho de la Universidad de Concepción, N° 205, año LXVII, Enero-Junio, año 1999, página 115.

garantía constitucional. Por lo demás y reiterando lo que hemos señalado, los datos de carácter personal no deben tener un trato de un bien cualquiera, siempre pertenecerán a sus titulares y son ellos quienes siempre deben imponerse de su ubicación y tener la última palabra con respecto al destino que se les dará.

También creemos que se debería consagrar en nuestra Carta Fundamental la **autodeterminación informativa**, a la cual ya hemos aludido, como un derecho fundamental. Este nuevo derecho se trata de fiscalizar la utilización de las informaciones personales independientemente si éstas pueden ser calificadas de íntimas, reservadas, secretas, privadas, ello nos permitirá al ciudadano controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo.

Unido a lo anterior se debe elevar a rango constitucional el instrumento que crea la ley para la protección de datos personales, llamado amparo en algunas ocasiones (art16, inc. 1° usa esa nomenclatura), como también reclamación en otras (mismo art. En la letra a), a fin que la autodeterminación informativa no sea una mera aspiración o declaración de buenas intenciones. Con ello se crea lo que en doctrina se denomina el Habeas Data.

En cuanto al organismo administrativo regulador del funcionamiento de las bases en manos de los organismos públicos creado por la Ley N° 20.285, denominado Consejo para la Transparencia consideramos que, si bien es cierto representa una avance, consideramos que limitarlo sólo a vigilar el cumplimiento de la Ley N° 19.628 por parte de los órganos de la administración del Estado es una cortapisa que sólo se justifica en un aspecto netamente práctico, esto es que se consideró prematuro dotarlo de los poderes suficientes para efectuar una fiscalización de amplio espectro que abarque a los privados, dejando para una etapa posterior una ampliación de su competencia. Esperamos que ésta haya sido la intención del legislador, ya que de lo contrario el Consejo habrá nacido herido en un ala, puesto que es en el mundo privado donde suelen efectuarse la mayor cantidad de reclamos por abusos en el tratamiento de datos personales.

La doctrina también estima que se deben consagrar dos derechos que la Ley N° 19.628 omitió y que existen en otras legislaciones:[65]

- <u>El derecho a impugnar valoraciones</u>, que consiste en la facultad concedida al titular de los datos para impugnar aquellos actos administrativos o decisiones privadas que impliquen la valoración de su comportamiento que se base exclusivamente en un tratamiento de sus datos personales que ofrezca una definición de sus características o de su personalidad. El objetivo que se pretende es impedir que el afectado quede sometido a los

[65] Anguita Ramírez, Pedro, "La protección de datos personales y el derecho a la vida privada", Editorial Jurídica de Chile, año 2007, página 304.

efectos jurídicos de una decisión que se base únicamente en el contenido de un fichero de datos que haya sido creado para evaluar determinados aspectos de su personalidad.

- El derecho de consulta, que consiste en la facultad de los titulares para solicitar y obtener gratuitamente de un registro general y público de la existencia de una base de datos, su finalidad y responsable.

En el aspecto infraccional estimamos que las penas de multas con que se sancionan algunas conductas (art. 16, letra h), como así también una eventual indemnización del daño patrimonial y moral que se causare por el tratamiento indebido de datos personales son medidas insuficientes para cautelar la protección de los datos personales, debiéndose proceder a la instauración de tipos penales relativos al tratamiento de datos personales con infracción a la ley, independizándolos del ámbito informático, ello porque el tratamiento de datos puede ser automatizado o manual.

Finalmente creemos que se debería explorar la posibilidad de que se establezca legalmente la criptografía[66] como mecanismo de resguardo en las transmisiones de datos, ya que es en ese momento en el cual las filtraciones e interceptaciones pueden tener mayor efectividad, logrando el apoderamiento de información proveniente de grandes bases de datos. Dichas bases de datos, al estar encriptadas, estarían protegidas de cualquier mal uso que el interceptador quiera darles. Con ello se cumpliría cabalmente lo estipulado en el art.5° de la ley.

Consideramos que con estas medidas lograríamos un estándar de protección mayor que el que actualmente existe, logrando colocar a nuestro país si bien no a la vanguardia en este tema, sin lugar a dudas no a la saga, como es el lugar que estimamos ocupa hoy Chile en cuanto a la protección de datos personales.

Una reflexión final: la protección de datos personales enfrenta hoy nuevos desafíos totalmente impensados una década atrás. El 11 de Septiembre de 2001 cambió para siempre los paradigmas que hasta ese momento se manejaban sobre el tema en los países desarrollados imponiendo un nuevo referente que se transformaría con el tiempo en una política ya aceptada a todos los niveles: la obsesión por la seguridad. Pero ¿dónde acaba esta obsesión?, no lo sabemos. Acuden a nuestra mente los nombres de los servicios de inteligencia de Stalin y de Hitler, los cuales utilizaron la información contenida en bancos o bases de datos en manos del aparato público de la época para efectuar las más brutales

---

[66] La **criptografía** es la parte de la criptología que estudia como cifrar efectivamente los mensajes. Su finalidad es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

represiones de que se tengan memoria sobre opositores políticos y minorías étnicas masacrando a millones de personas. Este ejemplo podrá parecernos un tanto melodramático y alejado de la realidad, pero ello no es así y para muestra tan sólo un botón: El Congreso de Estados Unidos otorgó a la central de inteligencia de su país (CIA) nuevos poderes legales para espiar a la gente en el propio territorio estadounidense, labor que hasta ese momento le estaba totalmente vedada. Ahora se permite a dicha agencia leer testimonios secretos ante los jurados de acusación sin la aprobación de un juez y obtener historiales privados de instituciones y corporaciones.

La situación antes descrita nos atañe directamente toda vez que en virtud de los tratados de libre comercio y de cooperación suscritos por Chile tanto con la potencia del norte como con países europeos nuestro gobierno ha debido poner a disposición de dichos países una gran cantidad de información referente a nuestro aparato productivo, por ejemplo estructura tributaria, antecedentes demográficos, organizaciones no gubernamentales, recursos naturales y, por supuesto, datos personales de la población en general. Ello representa un gran riesgo que en nuestra opinión no ha sido dimensionado en toda su amplitud.

Nosotros, los ciudadanos, hemos de mantenernos vigilantes e implicarnos en el asunto con el mayor interés. Con todo, la manera en que debemos mantenernos vigilantes es una cuestión problemática para la cual no existen soluciones mágicas. No obstante, creemos que una arquitectura legal moderna, de buena factura e inspirada en el principio de autodeterminación informativa que hemos esbozado, representa un escudo protector, si bien no absoluto, de gran ayuda a los ciudadanos para sentir confianza en que la información que versa sobre su vida privada se encuentra a buen recaudo.

Como se ha dicho "la confianza no es cosa que pueda crearse compulsivamente. No puede el hombre ser obligado a sentirse confiado".[67] Llevado esto a un análisis más específico al tema de autos, nos hace concluir que la fe pública que se ha depositado tanto en entes públicos como privados para la protección de datos personales debe ser objeto del mayor cuidado que sea posible, ya que es un bien demasiado valioso para permitir que se derroche de manera despreocupada. Ello porque representa, sin lugar a dudas, uno de los principales pilares que sirven de basamento y en el cual descansa el edificio republicano en que habita nuestra democracia.

[67] Palabras del orador, estadista y abogado norteamericano Daniel Webster (1782-1852).

BIBLIOGRAFÍA

1).- Textos.

1) Anguita Ramírez, Pedro, "La protección de datos personales y el derecho a la vida privada", Editorial Jurídica de Chile, año 2007.
2) Diccionario de la Real Academia de la Lengua Española, Microsoft ® Encarta © 1993-2007, Microsoft Corporation.
3) Ekmedkjián, Miguel Ángel, "Tratado Elemental de Derecho Constitucional", Tomo I, Buenos Aires, año 1993.
4) Escalante Gonzalbo, Fernando, "Derecho a la Privacidad", Instituto Federal de Acceso a la Información Pública, Méjico, Primera Edición, Marzo de 2004.
5) Frank Codd, Edgar, "A Relational Model Of Data For Shared", EE.UU., año 1970.
6) Frosini, Vittorio, "Cibernética, Derecho y Sociedad", Editorial Tecnos, Madrid, año 1982.
7) Historia Universal, Tomo 12, "La Era de las Revoluciones", Editorial Sol 90, Barcelona, España, año 2004.
8) Jijena Leiva, Renato, "Comercio Electrónico, Firma Digital y Derecho", Análisis de la Ley N° 19.799, Editorial Jurídica de Chile, Santiago, Chile.
9) Pérez Luño, Antonio – Enrique, "Del Habeas Corpus al Habeas Data", Madrid, Editorial Aranzi, año 1991.
10) Pérez Luño, Antonio – Enrique, "Ensayos sobre Informática Jurídica", Biblioteca de ética, filosofía del derecho y política, Madrid, España, Segunda Edición, año 2001.
11) Pfeffer, Emilio; Verdugo Mario y Nogueira Humberto, "Derecho Constitucional", Editorial Jurídica de Chile, año 1994.
12) Sagüés, Néstor Pedro, "Derecho Procesal Constitucional", Tomo III, "Acción de Amparo", Buenos Aires, año 1993.
13) Weiner, Tim, "Legado de Cenizas: La historia de la CIA", Editorial Random House Mondadori, Buenos Aires, Argentina, año 2008.
14) Whitaker, Reg, "El Fin de la Privacidad". Editorial Paidós, Barcelona, año 1999.

2).- Publicaciones.

15) Banda Vergara, Alfonso, "Manejo de datos personales. Un límite al derecho a la vida privada", Revista de Derecho Universidad Austral de Chile. Volumen XI, año 2000.

16) Bertelsen Repetto, Raúl, "Datos Personales: propiedad, libre iniciativa particular y respeto a la vida privada", cuadernos de extensión jurídica, Universidad de los Andes N° 5, año 2001.

17) Brandeis, Louis D. "Brandeis Dissenting". Opinión en el proceso "Olmstead vs. United States", año 1928.

18) Corral Talciani, Hernán, "De los derechos de las personas sobre los responsables de bancos de datos: El Habes Data chileno", cuadernos de extensión jurídica, Universidad de los Andes, N° 5, año 2001.

19) Corral Talciani, Hernán, "El derecho a la privacidad y los sistemas de tratamiento de datos personales en la Ley N° 19.628, Revista de Derecho de la Universidad de Concepción, N° 205, año LXVII, Enero-Junio, año 1999.

20) Herrera Bravo, Rodolfo, "Chile: Observaciones a las definiciones de la Ley N° 19.628, sobre protección a la vida privada", publicado en Alfa-Redi, revista de derecho informático, N° 105, Junio 2002, en http://www.alfa-redi.org/revista/data/49-8.asp

21) Herrera Bravo, Rodolfo, "La protección de datos personales como garantía básica de los derechos fundamentales", Revista de Derecho Público, Agrupación de Abogados de la Contraloría General de la República, año 2, n°5, Mayo/Agosto, 2001.

22) Jijena Leiva, Renato, "Ley Chilena De Protección de Datos Personales. Una visión crítica desde el punto de vista de los intereses protegidos", cuadernos de extensión jurídica, Universidad de los Andes N° 5, año 2001.

23) Magliona, Claudio, "Chile: Protección de Datos Personales. Políticas de Privacidad", publicado en Alfa-Redi, Revista de Derecho Informático, N° 101, Febrero 2002, http://www.alfa-redi.org/revista/data/45-3.asp

24) Mendoza Zuñiga, Ramiro Alfonso, "Régimen de los bancos de datos de organismos públicos. Una aproximación del Derecho Administrativo a la Ley Sobre Protección a la Vida Privada", cuadernos de extensión jurídica, Universidad de los Andes, N° 5, año 2001.

25) Nogueira Alcalá, Humberto "Autodeterminación Informativa y Habeas Data en Chile e Información Comparativa", biblioteca jurídica virtual del instituto de investigaciones jurídicas de la Universidad Nacional Autónoma de Méjico, página 458 (www.juridicas.unam.mx)

26) Rajevic Mosler, Enrique "Una vuelta de tuerca en materia de acceso a la información", publicado en www.fundaciónproacceso.cl, año 2008.

27) Reusser Monsálvez, Carlos, "Privacy, Risarvatessa, Intimidad y Autodeterminación Informativa", Apuntes para la discusión. Foro Digital, año 2001.

28) Vásquez Márquez, José Ignacio, “Análisis crítico sobre la naturaleza jurídica de la ley de protección a la vida privada”, Revista de Derecho de la universidad Finis Térrae, año III, N°3, año 1999.
29) Vial Claro, Felipe, “La Ley N° 19.628 Sobre Protección de Datos de Carácter Personal, Una Visión General”, cuadernos de extensión jurídica, Universidad de los Andes, N° 5, año 2001.
30) Warren, Samuel y Brandeis, Louis D., “The Right to Privacy”, Harvard Law Review, EE.UU., año 1890.
31) Wells Branscomb, Ann, “Who Owns Information?, From Privacy To Public Acces”, Basic Books, a division of Harper Collins Publishers, Inc., año 1994, página 29. Traducción del abogado argentino Leonardo Ghigliani, extraído de http://visitweb.com/leonardoghigliani.

3).- Recursos en Internet adicionales.

www.bcn.cl
www.emol.com