Dominios, Marcas y Comercio Electrónico en Internet

RENATO JAVIER JIJENA LEYVA

Profesor e investigador de Derecho Informático

Dominios, Marcas e "Identidad Empresarial".

Los nombres de dominio son las direcciones que permiten ubicar sitios en Internet, a pesar de que detrás de cada dirección hay un número único (URL) o identificador IP que registran los ordenadores, y son esenciales para mantener cierto mínimo orden indispensable en el ciberespacio.

Ellos, alfabetizados para facilitar su manejo y recordación poseen una o varias denominaciones particulares y una genérica o superior llamada de "top level" que va al final, y que puede ser geográfica o nacional (.cl para Chile, .fr para Francia, .es para España, etc.) o temática (.org para organizaciones, .net para las redes y .com para las comerciales). Así por ejemplo serán nombres de dominio los siguientes: "www.acti.cl"; "www.eanchile.cl", "www.ucv.cl"; "www.ompi.org"; etc.

Lo que se busca es identificar las diversas direcciones virtuales mediante dominios o nombres generalizados, que son geográficamente

independientes o transnacionales, que tienen un valor de mercado o económico y que pueden además constituir una "marca" susceptible de aprovechamiento comercial. Por cierto, no se trata de asuntos de menor cuantía. Así por ejemplo el dominio "business.com" fue vendido recientemente por la suma de 7.5 millones de dólares, convirtiéndose así en el más costoso de la historia. Hasta hace poco estaba registrado a nombre de un empresario inglés que hace tres años lo había adquirido a su propietario original por la suma de 150.000 dólares.

El enfoque del tema ha cambiado. Ya no podemos visualizarlo como la mera identificación técnica de ordenadores interconectados, sino que se trata de que toda entidad, empresa o persona natural que quiera mantener una página WEB u ofrecer comercialmente sus productos en Internet pueda tener debidamente inscrita y resguardada la dirección virtual de su sitio.

Recordado es el caso de un particular que presentó ante el Departamento de Ciencias de la Computación (DCC) de la Universidad de Chile una solicitud de registro, en orden a constituirse en asignatario o "propietario virtual" de 119 nombres de dominio en Internet. Dichos nombres individualizaban a entidades públicas y privadas, a Órganos del Estado y a entidades financieras, a personas jurídicas y a personas naturales, muchas de los cuales tenían registradas las marcas comerciales respectivas. El perjuicio era evidente: de haberse asignado los dominios aquellas no habrían podido instalar páginas "WEB" con sus marcas corporativas sin previamente negociar con el titular del registro.

La ley de Propiedad Industrial chilena establece que el titular de una marca comercial es propietario de la misma y que se encuentra facultado para usarla en forma exclusiva. La lógica indica que dicho titular también tiene el derecho de propiedad sobre la marca proyectado en Internet o virtualmente, a pesar de la "aterritorialidad de la red", debiendo tener la primera opción para inscribir el dominio o dirección a su nombre. Pero tal facultad sólo podría alegarse y hacerse valer con facilidad en Chile y sólo respecto a la denominación de top level ".cl", atendida la vigencia territorial de la ley sobre propiedad industrial que, a priori, no podría pretender tener aplicación fuera de nuestro territorio jurisdiccional.

En definitiva, se trata de proteger lo que un abogado y una empresa especializada han denominado la "identidad empresarial" o la "identidad comercial" de una empresa, producto o servicio, esto es, uno de los más importantes activos intelectuales que surge a partir de las distintas experiencias que los consumidores tienen para percibir y posicionar una marca. Efectivamente, como se afirma, los dominios son hoy portadores de la identidad comercial de toda empresa y tienen un valor estratégico, y en ellos puede cristalizar -digamos gran parte- del posicionamiento, prestigio y trayectoria de una organización.

Lineamientos de la IANA y la ICAAN.

La existencia de un ente que controle el sistema de asignación de nombres de dominio en Internet es un tema complicado. A instancias de la IANA o Internet Assigned Numbers Authority, un organismo contratado por el Gobierno de EE.UU. para administrar técnicamente el sistema de direcciones de la red y mantener un "Registro de Nombres de Dominio", en un comienzo países como EE.UU. declararon urbi et orbi ser partidarios de la autoregulación.

Pero en la práctica y reteniéndose de facto un servicio de carácter internacional, se cedió mediante un contrato de exclusividad a una empresa vinculada al Departamento de Defensa y a la CIA -Network Solutions Incorporate- el monopolio para que se registren y asignen y para que se mantenga un control exclusivo de los dominios más extendidos o que identifican a la mayoría de los actores de Internet (aquellos con denominaciones de top level temática, .com, .net, y .org). Tal opción, contenida en un primer documento conocido como "Green Paper", fue resistida por grupos académicos y técnicos interesados y proveedores como la "Internet Society", quienes reclamaron la necesaria creación de una entidad sin fines de lucro que se hiciera cargo de la tarea.

La IANA preparó un segundo borrador de propuesta o "White Paper", en general relacionado con el comercio electrónico global y, en particular, sobre un nuevo modelo de administración de nombres de

dominio en que el proceso de registro es competitivo y no monopólico para Network Solutions, porque se postuló crear siete nuevos dominios genéricos y temáticos que serían administrados por diversas empresas repartidas en distintos lugares del mundo. El documento, suscrito por varias entidades vinculadas a Internet bajo la legislación de Suiza, contempló además la creación de un nuevo ente coordinador global de consenso, sin fines de lucro y formado por entidades privadas conocido inicialmente como Comisión de Servicios Públicos de Internet y denominado en definitiva, en Octubre de 1998, como "Internet Corporation for Assigned Names and Numbers" o ICANN.

El Reglamento del NIC Chile (www.nic.cl).

Este tema ha dado pie a la existencia de un importante grado de regulación jurídica en la red, para ser más exactos -y esto es novedoso-, de autoregulación. Las reglamentaciones que ha elaborado la IANA en orden a mantener un "Registro de Nombres de Dominio" han sido acogidas internacionalmente en forma mayoritaria.

Por cierto, también se ha sostenido con cierto fundamento que el sistema sea administrado en cada país por el mismo órgano encargado del registro de marcas y patentes comerciales, pero esto enfrenta al menos dos problemas: que existen dominios que se asignan y registran para tener vigencia en todo el mundo y por sobre los territorios jurisdiccionales geográficos (.org, .com, .net); y que conllevaría dictar nuevas leyes e inventar nuevos procedimientos administrativos para la asignación, el registro y para la solución de controversias -en desmedro del mecanismo del arbitraje que es, evidentemente, el más idóneo-.

Actualmente en Chile se asignan e inscriben los dominios ".cl" en un registro que administra el Departamento de Ciencias de a Computación (DCC) de la Universidad de Chile. Allí funciona el Centro de Información de Redes (en inglés NIC). El Reglamento elaborado al efecto es una normativa autoacordada o autoestablecida, que no ha sido promulgada en Chile por autoridad alguna y por ende no publicada en el Diario Oficial (no cabe presumirla legalmente conocida por todos), sino que es aceptada y

acatada de hecho por los usuarios de Internet. Jurídicamente esto es novedoso porque se trata de una voluntad colectiva que autónomamente acepta determinadas normas, aunque hay quienes sostienen que todo asignatario en definitiva lo que hace no es sino celebrar un contrato de prestación de servicios con el NIC respectivo.

En un principio no se estableció relación alguna con las marcas que registra el Ministerio de Economía, pero posteriormente se agregó al Reglamento una instancia de arbitraje obligatorio en el caso que dos personas o empresas reclamen un mismo nombre, debiendo el mediador o el árbitro, necesariamente, considerar la existencia de "marca preexistente" al decidir quien tiene el mejor derecho de usar un dominio.

El caso ONDAC.

Por la vía del Recurso de Protección, que es una acción cautelar que ampara determinadas garantías constitucionales frente a actos arbitrarios o ilegales, en 1998 una empresa proveedora de software -Ondac Chile Ltda.-, que había registrado previa y debidamente en el Ministerio de Economía la marca "Ondac", recurrió en contra de la Universidad de Chile por haberse registrado o asignado en el DCC el dominio "ondac.cl" a otra empresa que no tenía derechos preexistentes. El mecanismo constitucional se utilizó amparándose legalmente en la normativa de la ley de propiedad industrial y en la CPE. de 1980, ante la negativa del ente universitario de registrar o asignarle el nombre de dominio a la primera por haberlo solicitado previamente la segunda en conformidad al Reglamento ad hoc.

El recurso fue declarado sin lugar en la Corte de Apelaciones: a) debido a que el DCC sólo cumplió con la reglamentación vigente y el recurrente no formuló oposición en los plazos que contempla el Reglamento; b) a que, en opinión del Tribunal, al DCC no cabía exigirle al momento de asignar un dominio un juicio o pronunciamiento respecto del alcance de la protección que se le otorga a las marcas comerciales registradas (se habría arrogado una potestad jurisdiccional ajena); y, c) a que el conocimiento de este tema no era propio de un recurso de protección.

No obstante que el DCC nunca pretendió arbitrariamente perjudicar a la empresa Ondac, el criterio del Tribunal es errado y producto de un análisis meramente formal. La Corte no entró al fondo del asunto. En la especie no cabía desconocer la aplicación de la ley de propiedad industrial, ni la procedencia del recurso de protección para detener en Chile y preventivamente (sin perjuicio de hacer valer otros derechos o reclamar conforme a la ley de propiedad industrial) una conducta perjudicial y atentatoria contra la garantía constitucional del derecho de propiedad, máxime cuando el Reglamento no puede considerarse una "ley especial" sino que es una normativa autoacordada o autoestablecida que no ha sido promulgada por autoridad alguna y que, hasta antes de contemplar un mecanismo obligatorio de arbitraje, podía lesionar los derechos de los titulares de las marcas comerciales.

Sanción a los "cibercuatreros".

En EE.UU. dos texanos registraron una larga lista de nombres de dominio que incluían la palabra "microsoft", específicamente los nombres "microsoftwindows.com" y "microsoftoffice.com"; posteriormente solicitaron entre 50 y 100.000 dólares a la transnacional del software. Microsoft accionó legalmente por haberse infringido las marcas comerciales de la empresa y confundido a los usuarios. A la luz de estas prácticas, el Congreso de Estados Unidos aprobó una ley que sanciona penalmente a todos aquellos que, dolosamente y sin tener fundamento, intenten registrar como nombres de domino marcas comerciales pertenecientes o previamente inscritas por otras compañías. Esto será aplicable, por cierto, siempre y cuando el hecho doloso ocurra dentro de EE.UU.

El Reglamento del NIC chileno también acaba de ser modificado para regular este tema, estableciéndose que serán acogidos los criterios de la ICANN que permiten revocar la inscripción de dominios cuando se compruebe que se realizaron de mala fe. Por ende, quedó sin efecto, por atentarse contra la tutela del derecho de marcas, la norma cerrada del Reglamento que establecía que una vez inscrito un nombre de dominio ya no podía acogerse otra solicitud de registro por el mismo simplemente por razones de plazos vencidos u oportunidad.

Se han presentado en nuestro país casos de personas que a través de Internet han registrado en EE.UU. nombres de dominios con las extensiones ".net", ".com" y ".org" relacionadas con empresas chilenas. Cualquier acción legal de reclamo sólo podría intentarse conforme a la legislación del país Norteamericano o la reglamentación de Network Solutions, porque es dentro de su territorio jurisdiccional donde se produce el hecho del registro. Que la magia de Internet permita presentar una solicitud y obtener un registro de dominio en el extranjero desde o sin moverse de Chile no significa, como han creído algunos abogados anclados al derecho tradicional, que sea factible interponer en nuestro país una acción de reclamo civil o penal en relación a hechos acaecidos fuera de nuestro territorio.

Lo anterior fue entendido por la empresa Chilnet S.A., que a fines de 1998 ganó en primera instancia una demanda interpuesta en EE.UU contra los representantes de una compañía israelita que inscribió a su nombre los dominios "chilnet.com" y "chilnet.net", en el administrador de los dominios ".com" y ".net" de EE.UU. A quien solicitó la inscripción de los dominios la empresa se le hizo presente que bajo el Domain Name Registration Agreement (www.internic.net/help/agreement.txt) tenía que basarse en las pláticas de disputas suscritas en el sitio WEB del administrador de dominios, conforme a las cuales debía traspasar las inscripciones a la empresa chilena. Ante la negativa se realizó una presentación formal, con lo cual se obtuvo que la entidad reguladora bloqueara la petición de registro de dominios hecha por la empresa israelita y acogiera la petición de detener o dejar en espera -retroactivamente- el uso de los mismos.

ANEXO:
LA NUEVA LEY CHILENA SOBRE LA NO PROTECCIÓN DE DATOS PERSONALES, Nº19.628, del 28 de Agosto de 1999

I. INTRODUCCIÓN.

Si bien es cierto el problema de la protección legal de datos personales frente al tratamiento computacional de los mismos es un tema con bastante perspectiva en países extranjeros, en Chile constituye una realidad desconocida y poco estudiada jurídicamente. Digamos desde ya que este tema, el de los *"datos personales o nominativos procesados computacionalmente"* va mucho más allá que el problema de los protestos, de la morosidad comercial y de los archivos históricos almacenados en bancos de datos.

Para un adecuado análisis de la ley en comento se ha estimado necesario realizar en el informe el siguiente desarrollo expositivo:

En el **Capítulo II** se plantean los elementos conceptuales y doctrinarios necesarios para entender cuál es el problema de fondo que pretende solucionar el denominado *"Derecho de la Protección de Datos";*

En el **Capítulo III** se sistematizan cuáles son las situaciones de hecho y los elementos jurídicos que, conforme a la realidad y la legislación chilena, deben tenerse presente para abordar el tema;

En el **Capítulo IV**, recogiéndose los elementos previamente expuestos se revisa brevemente cuál fue la tramitación parlamentaria de la ley aprobada y cuál es el contenido y los alcances de los artículos que la conforman, para cerrar los comentarios formulando algunas observaciones generales a la ley; y,

Se incorpora en el **Capítulo V** el texto de la ley.

II. LA PROTECCIÓN DE DATOS PERSONALES O NOMINATIVOS Y EL "HABEAS DATA". PLANTEAMIENTOS DOCTRINARIOS Y DERECHO COMPARADO.

1. Generalidades.

Suele afirmarse que el abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la intimidad, porque cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados. Esta imagen inmaterial del titular de los datos debe ser resguardada porque puede ser creada errada o dolosamente, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio.

Conceptualmente, un dato es un antecedente que da cuenta de un hecho o de una característica determinada. El conjunto organizado de datos constituye información y, sociológicamente hablando, un nuevo bien económico de alto valor y una forma de poder.

Un dato es personal o nominativo cuando permite identificar cualquiera 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, las operaciones comerciales que se realizan, las acciones en empresas que se poseen, los depósitos en cuenta corriente o a plazo, los impuestos pagados, etc.

2. El problema de fondo se origina por un conflicto entre dos intereses relevantes.

Por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas,

su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc.

Por el otro, un interés -también muy legítimo- que poseen los gobiernos y los particulares para acceder a cierta información: ... los Estados para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quienes tienen SIDA al momento de fijar políticas de salud; y los particulares, generalmente constituidos en empresas de servicios o entidades gremiales, que 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.

Se trata, por ende, de lograr un equilibrio y establecer límites entre el derecho a la intimidad que consagra el artículo 19N°4 de la Constitución y un derecho a la información -consagrado en el artículo 19N°12- fundado en razones de orden público.

La interrogante a dilucidar o la hipótesis de trabajo, en consecuencia, puede ser la siguiente: ¿cómo conciliar el Derecho a la Información con el Derecho a la Intimidad?; ¿cómo equilibrar por un lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad?. Se trata de una cuestión importante por cierto, no de meras disquisiciones teóricas o doctrinarias, porque si bien es cierto el orden público social y económico de una Nación requiere que tanto el Estado como los particulares manejen determinados datos personales, sea para fijar políticas de salud o para evitar la morosidad comercial, esto no puede traducirse, al extremo, en abusos contra las personas. Así ha ocurrido con la información comercial o sobre los antecedentes patrimoniales de los chilenos, que en base a inexistentes argumentos legales o erradas interpretaciones constitucionales hasta antes de la ley era procesada y comercializada sin límite alguno[1] y hoy en día, al

[1] Con ocasión de la interposición de recursos de protección en contra de la empresa DICOM S.A. se ha argumentado, sobre la base de interpretar las Actas de la Constitución de 1980 pero sin fundamento serio, que la Carta Fundamental distinguiría entre un ***patrimonio moral*** y un ***patrimonio económico*** de las personas; por ende -lo que es un aburdo y una falacia, porque el debate nunca fue abordado por el Constituyente y porque entre los años 1977 y 1979 el problema del procesamiento computacional de datos personales no existía-, ciertos datos que

tenor de la nueva ley aprobada que se informa, se hace con límites mínimos o meramente formales.

La respuesta doctrinaria ha sido la formulación de un nuevo concepto del 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 ser dejado a solas"); 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.

3. *"Derecho de Acceso o Habeas Data".*

Se produce -doctrinaria y legalmente- la conciliación entre el Derecho a la Intimidad y el Derecho a la Información a través del control que para el titular de los datos posibilita el denominado ***"Derecho de Acceso"*** o ***"Habeas Data"***, una nueva garantía fundamental (o un nuevo mecanismo de resguardo y tutela) que contemplan en el Derecho Comparado tanto algunas Cartas Fundamentales como las llamadas Leyes de Protección de Datos, y una consagración del ***"Principio de la Autodeterminación Informativa"***.

El *"Habeas Data"* es una acción cautelar de rango constitucional, heredera de otro recurso y tan importante como el *"Habeas Corpus"*, que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales -al decir de una sentencia histórica del Tribunal Constitucional alemán- "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente.

---

conformarían el primero serían reservados y el segundo comprendería toda la información comercial/nominativa que sería pública, tendiendo la sociedad derecho a conocerla y DICOM a recopilarla, procesarla, cruzarla y comercializarla.

Atendida la relevancia de este *"Derecho de Acceso"* él ha sido consagrado en tratados internacionales y en Constituciones como las de Portugal, España, Paraguay y -en 1994- en Argentina, considerándosele como un instituto del derecho procesal constitucional del que conocen órganos autónomos ad hoc y los Tribunales Superiores de Justicia. Porque de lo que se trata es de proteger la intimidad de las personas.

4. *¿Cómo logran las Leyes de Protección de Datos, vigentes desde hace 20 años en el Derecho Comparado, el equilibrio de los intereses involucrados?.*

Básicamente de la siguiente forma: no niegan la posibilidad del procesamiento o tratamiento de datos, pero consagran facultades de acceder, corregir, actualizar o eliminar datos para los titulares de los mismos (enmarcadas en el denominado *"Habeas Data"*); establecen mayores limitaciones para el procesamiento cuando los datos son de especial relevancia como los llamados "sensibles" o "personalísimos" (vida sexual, salud, raza, credo religioso, filiación política, etc); regulan separadamente el procesamiento que realice un órgano público, una persona natural o una persona jurídica, estableciendo diferentes requisitos de constitución; regulan acabadamente las obligaciones y prohibiciones del responsable de un sistema; la operatividad de todas las normas descansa en un órgano autónomo de control y fiscalización, "a priori" -autorizando a procesar y fijando los requisitos para hacerlo- y "a posteriori" -conociendo de los reclamos y sancionando-; y configuran sanciones administrativas como multas y penales -tipifican delitos- para el caso que las normas de la ley no se cumplan.

III. EL PROCESAMIENTO O "TRATAMIENTO" COMPUTACIONAL DE DATOS PERSONALES O NOMINATIVOS EN CHILE. LOS ANTECEDENTES SOBRE SOLVENCIA PATRIMONIAL.

1. *Procesamiento de datos personales en los sectores público y privado.*

Los cotidianos atentados contra la privacidad de los chilenos, tanto en cuanto datos personales o nominativos tratados mediante sistemas informáticos, desde hace bastante tiempo vienen cometiéndose por órganos

estatales y por empresas comerciales, en particular por éstas últimas. Porque uno de los temas que subyace en este debate es la necesidad de regular un gran negocio económico que vulnera derechos fundamentales de las personas, como la vida privada, el acceso al crédito, la libertad de trabajo, la libre iniciativa en materia económica y la igualdad ante la ley.

Existen sectores gremiales y empresariales que incluso sostienen, y es una falacia, *que la mayoría de las personas no se oponen a entregar su información mientras obtengan algo a cambio.* Más falso aún es sostener que no debemos preocuparnos por la defensa de la privacidad de los chilenos, porque el tema se ha trasladado a una "negociación" donde los consumidores pedirán recompensa por proporcionar sus datos, ante lo cual el procesamiento de datos personales o nominativos debiera quedar entregado a una autoregulación.

Existen empresas que lucran con la insolvencia patrimonial de los chilenos -es su único fin-, "Abusando del Derecho" o actuando bajo una legalidad meramente formal o aparente (hasta la aprobación de la ley que ahora se informa), que elaboran perfiles de personalidad y comportamiento económico, y que han inventado argumentos legales como aquél que según la Constitución de 1980 existirían dos patrimonios para cada persona, uno moral y otro económico, siendo privado el primero y público el segundo, argumento legal definitivamente cuestionable e infundado que, lamentablemente, ha encontrado acogida en el desconocimiento de los Tribunales Superiores de Justicia quienes se han manifestado por la vía del conocimiento y fallo de algunos Recursos de Protección.

2. *La propiedad de los datos.*

También en Chile varias multitiendas comerciales exigen, al momento de otorgar créditos y facilidades de pago, una serie de datos que posteriormente almacenan computacionalmente; pública y gremialmente han vindicado la propiedad de dicha información. Una empresa chilena que ofrece productos de bases de datos en Internet (v.gr. guías de empresas) advierte en su página WEB que está otorgando el derecho de accesar a sus bases exclusivamente a modo de consulta, que bajo ninguna circunstancia

puede arrendarse o venderse parte o toda la información recopilada y ofrecida, y *que el contenido de las bases de datos es de su propiedad y está protegido por el derecho de autor.* Estas afirmaciones constituyen un gran error jurídico, toda vez que son cosas muy distintas *"el continente"* o la estructura de la base o banco de datos que *"el contenido"* o la información almacenada en el mismo.

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 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°), establecen claramente 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".

3. Los datos personales-patrimoniales o sobre solvencia patrimonial.

En materia de datos personales-patrimoniales o sobre solvencia patrimonial, podía sostenerse que la regla general del ordenamiento jurídico chileno era -hasta antes de la ley aprobada- su reserva y confidencialidad.

Es muy importante destacar que en Chile no existía norma legal alguna que estableciera que los antecedentes patrimoniales o comerciales de las personas que obran en poder de bancos y entidades financieras, de AFP e Isapre, de la Tesorería General de la República, del SII, del INE -entre otros- eran públicos. Muy por el contrario, la relevancia y naturaleza confidencial o reservada que nuestro ordenamiento jurídico positivo otorgaba (hasta antes de la ley) a la información comercial, bancaria y tributaria y la tendencia a lograr su resguardo legal, queda de manifiesto por la consagración constitucional o legal de las instituciones del secreto bancario, del secreto tributario y del secreto estadístico, los cuales deben ser especialmente observados por los órganos estatales y las instituciones financieras pero que también obligan a los particulares.

3.1 *Sobre la necesidad de publicitar los antecedentes comerciales o patrimoniales "negativos" y su fundamento constitucional.*

A nivel de principios jurídicos los únicos antecedentes económicos, comerciales o financieros que una sociedad requiere conocer para mantener el Orden Público Económico son aquellos que sean negativos o que den cuenta de conductas comerciales, bancarias o tributarias irregulares (incumplimiento de obligaciones dinerarias), como es el caso de los protestos de documentos mercantiles o la constitución en mora en el pago de las deudas[2].

IV. ANÁLISIS DE LA LEY APROBADA.

A. DEBATE PARLAMENTARIO PREVIO A LA LEY.

1. *La Moción del ex senador señor Eugenio Cantuarias, sobre proteccion "civil" de la vida privada.*

La indicación de Cantuarias -de 1992- nunca pretendió ser una ley de protección de datos personales o nominativos. Antes, muy por el contrario, el ex Senador consignó expresamente que sólo buscaba resaltar algunos principios fundamentales para aproximarse al tema y que la materia debía ser abordada en otro proyecto más acabado. Su moción, fundada en una ley similar española, era un ***proyecto de ley sobre protección "civil" de la vida privada***, bien jurídico que debía ser resguardado ante lo que él llamaba "intromisiones ilegítimas".

[2] La realidad cotidiana en Chile ha llegado a tal extremo que se han suprimido las gestiones notariales previas y las judiciales para notificar el protesto de documentos, bastando sólo que una empresa haga llegar a DICOM un listado de deudores -¡a veces atrasados en el pago de una cuota de TV cable!- para que dichos antecedentes sean publicitados. A este respecto, el *artículo 17º* de la ley veremos que legaliza la publicación de datos sobre mera morosidad comercial o atraso en el pago de una cuota de una deuda, sin necesidad de protestar documento mercantil alguno.

Los 26 artículos se distribuían en 5 Títulos, sobre disposiciones generales el I, sobre protección de datos el II (artículos 8 a 13), de las intromisiones ilegítimas el III (una de ellas mediante medios tecnológicos como la informática), de las acciones civiles el IV y sobre tribunal competente y procedimiento el Título V.

2. *El proyecto aprobado por el Senado en Octubre de 1995.*

El texto de la moción se redujo a 16 artículos ordenados en 4 Títulos. El Título I sobre disposiciones generales -artículos 1° a 4°- estableció, aludiendo a garantías o derechos distintos como son la privacidad, la imagen y el honor, el amplio ámbito de aplicación de la ley, a saber, "el respeto y protección a la vida privada y a la honra de la persona y su familia". Propuso un alcance legal para "la vida privada"; establecía que las sentencias judiciales no podían fundarse en intromisiones ilegítimas; y, consagró una obligación del secreto estadístico.

El Título II, "de la protección de datos", en apenas 5 artículos -5° a 9°- efectivamente sólo sentaba algunos principios fundamentales sobre el tema, relacionados con la no desviación del fin para el cual se procesan los datos, con la obligación de informar sobre qué datos se tienen almacenados, con el Derecho de Acceso o conocer cuáles son los datos procesados, además de rectificarlos, completarlos, aclararlos actualizarlos o suprimirlos, y establecía expresamente un derecho a la indemnización de perjuicios inclusive por concepto de daños morales.

En los artículos 10°, 11° y 12° el Título III declaraba ampliamente qué constituía una intromisión ilegítima en la vida privada "todo acto u omisión arbitrario o ilegal que perturbe, amenace o prive a una persona del ejercicio legítimo del derecho a su vida privada".

El Título IV aludía a acciones, procedimientos y competencias para conocer los casos de infracciones a la ley, estableciendo expresamente, lo que era un aporte antes discutido doctrinaria y jurisprudencialmente, la obligación de indemnizar el daño moral.

3. *Modificaciones introducidas al proyecto de ley en la Camara de Diputados: ...un equivocado intento por legislar en materia de proteccion de datos personales.*

La Cámara de Diputados estimó, en segundo trámite constitucional, que lo más relevante del proyecto aprobado por el Senado eran las normas sobre protección de datos personales.

En consecuencia, y en vez de aprobar un texto relativamente simple y genérico como el enviado desde el Senado, intentó elaborar un cuerpo legal integral sobre el tema y buscó promulgar en Chile una ley de protección de datos, a la manera de textos del Derecho Comparado como las leyes francesa de 1978 y española de 1992. De poco sirve pues analizar un texto comparado entre el proyecto aprobado por el Senado y el modificado en la Cámara, porque caminaban por rumbos distintos.

Creemos que el texto propuesto como tal fue equívoco, ambiguo, confuso, asistemático, parcial e insuficiente, tanto por sus errores de forma como de fondo, y así lo hicimos ver en un informe presentado en Mayo de 1998 a solicitud del Presidente de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado.

4. *El texto aprobado por el Senado en 1998 (tercer trámite constitucional). Proposición para ser debatida en Comisión Mixta.*

Para el solo efecto de zanjar las discrepancias que surgieron en relación al texto aprobado por la Cámara previamente, la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado elaboró un nuevo texto y recomendó someterlo a consideración de una Comisión Mixta.

B. CONTENIDO PRINCIPAL DE LA LEY APROBADA EN DEFINITIVA POR LA COMISIÓN MIXTA.

1. *Estructura y contenido o ideas matrices de la ley.*

La Ley consta de un **Título Preliminar** sobre "Disposiciones Generales" (artículos 1°, 2° y 3°); de un **Título I** sobre "la utilización de datos personales" (artículos 4° al 11°); de un **Título II** sobre "derechos de los titulares de datos" (artículos 12° a 16°); de un **Título III** acerca de "la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial" (artículos 17° a 19°); de un **Título IV** sobre "tratamiento de datos por organismos públicos" (artículos 20°, 21° y 22°); de un **Título V** acerca "de la responsabilidad por las infracciones a esta ley" (artículo 23°); de un **Título Final** que modifica el Código Sanitario (artículo 24°); y de tres **Disposiciones Transitorias.**

En esencia, existen "datos personales" o nominativos que le pertenecen a sus titulares y que son "tratados" manual o automatizadamente, tanto por órganos públicos como por empresas o personas particulares, a quienes la ley califica como "responsables del registro o banco de datos".

La regla general formalmente declarada por el texto legal es que dicho "tratamiento de datos personales" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" (por lo cual no se requiere de autorización para su tratamiento) y se consagran importantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera declaración de principios.

El mecanismo de resguardo recogido parcialmente del Derecho Comparado se denomina "Derecho de Acceso" o "Habeas Data", y éste, después de ejercerse ante quien aparezca como responsable sólo puede reclamarse ante los tribunales ordinarios de justicia.

2. *Ámbito de aplicación.*

A este respecto, el *artículo 1°* establece que se sujetará a las disposiciones de esta ley ***el tratamiento de los datos de carácter personal***, definidos por el *artículo 2ª* como los relativos a cualquier información concerniente a **personas naturales** identificadas o identificables, contenidos en registros o bancos de datos y procesados tanto por organismos públicos como por entidades particulares.

No estamos frente a una ley relacionada sólo con el procesamiento computacional de datos. Porque el *artículo 1°* no utiliza la expresión "tratamiento automatizado", y porque la letra o) del artículo 2° define muy ampliamente como "tratamiento de datos" a "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no...", claramente quedan comprendidos aquí todos los registros, kardex o ficheros manuales o soportados en papel, por cierto, hoy en día de menor importancia cualitativa y cuantitativa que los registros informáticos.

Como corolario y sentando algo así como un principio de legalidad o una especie de condición general de licitud para este ámbito, agrega el *artículo 1°* que cualquier persona podrá efectuar el tratamiento de datos personales siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico, y que en todo caso se deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

2.1 *Situación de las personas jurídicas como titulares de datos o sujetos de tratamiento automatizado.*

Nada dice la ley respecto a los datos "personales" de las personas jurídicas, las que también poseen atributos de su personalidad, aunque su naturaleza jurídica emane de una ficción legal. Ellas son sujetos de información cuyos antecedentes también son "tratados"

computacionalmente, y por definición quedan al margen de la ley que sólo rige en relación a "titulares" personas naturales.

Debe reconocerse que el punto no es unánime sino discutido en el Derecho Comparado, sobre todo para quienes consideran que existen otros mecanismos jurídicos para resguardar los atributos de las personas jurídicas, a saber, el derecho de sociedades, las leyes sobre propiedad industrial e intelectual, las normas sobre libre competencia, etcétera, todas las cuales, empero, de manera alguna resguardan el eventual tratamiento abusivo que se haga por las empresas que prestan servicios de información.

Ocurre que la información sobre las personas jurídicas es tan relevante como la de las personas naturales y también merece ser resguardada. Esta tutela jurídica por ende permanece en el ámbito de las reglas generales del derecho, por lo que cualquier persona jurídica respecto de la cual se abuse de sus antecedentes propios o bien éstos sean procesados en forma errada (datos obsoletos, caducos, inexactos), deberá recurrir a los procedimientos, acciones y recursos generales contemplados en nuestro ordenamiento jurídico. Estimamos que si bien en menor amplitud que las personas naturales, las personas jurídicas también gozan de un necesario derecho a la confidencialidad o reserva de los antecedentes que a ellas se refieren, por cuanto éstos las convierten en sujetos de derechos y en personas identificadas e identificables. En la realidad actual del procesamiento de datos, no se explica como el legislador no consideró de manera alguna esta situación.

2.2 *Ámbito de aplicación de la ley desde la perspectiva de los "Responsables de las Bases de Datos".*

La Ley distingue lo que es el procesamiento de datos personales al interior de la Administración Estatal o en el Sector Público y lo que ocurre en el sector privado o respecto al tratamiento por particulares, sean éstos personas naturales o jurídicas.

Todas las leyes de protección de datos en el Derecho Comparado establecen una clara diferenciación entre lo que son las bases de datos

"públicas" y las "privadas", en atención a la naturaleza de la entidad que las administra y no, como lo hace la ley chilena, en consideración a la fuente de la información o al tipo de datos procesados.

2.2a) El artículo 2° letra k) define lo que son los Organismos Públicos, entendiendo por tales a *"las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado".*

Respecto a las ***bases de datos públicas o administradas por organismos públicos***, la ley contempla un Título específico -el IV-, compuesto por los artículos N°20, 21 y 22.

Para efectos de este informe cabe indicar que el *artículo 22* contempla la obligación de que sea el Servicio de Registro Civil el ente que llevará un Registro Público de Bancos de Datos, pero sólo en relación a entes estatales y excluyendo de la obligación de registro a las empresas particulares. Esta disposición, fruto de una indicación presentada por el Ejecutivo durante el debate en Comisión Mixta ya que se trata de una materia de iniciativa exclusiva del Presidente, es de difícil comprensión, porque en sí no lleva envuelta el establecer una instancia o grado de fiscalización alguno, que es la razón de ser en las leyes de protección de datos de la existencia de órganos ad hoc[3]. ¿Cuáles son las sanciones a aplicar al órgano público que no se registre?; ¿puede el Servicio de Registro Civil realizar algún control al efecto y con qué facultades, si en Derecho Público sólo puede hacerse aquello que esté expresamente permitido?.

Nunca se entendió la importancia de que la ley contemplara un órgano de fiscalización y la existencia de un registro ad hoc. Inicialmente no se abordó el tema bajo el débil argumento de "no querer ser burocráticos";

[3] Para entender la importancia y la operatividad práctica del tema, véase en Internet la dirección *www.ag-protecciondatos.es/regis.html,* que conecta con el Registro General de Protección de Datos existente desde 1992 en España.

posteriormente se propuso que fuera la Contraloría General de la República[4]; luego se estableció (en el proyecto aprobado en el Senado) que sería un órganismo público el encagado de llevar un registro de los bancos de datos tanto públicos como privados; la solución final elaborada en la Comisión Mixta para hacer el sistema aún menos restrictivo para las empresas dedicadas al procesamiento de información, es insuficiente, porque ni siquiera incluye la obligación de registro para empresas o personas privadas.

2.2b) Respecto a las ***bases de datos administradas por entidades particulares*** no ocurre lo mismo, especialmente porque la ley excluyó toda obligación de que los responsables de las mismas estén anotados en algún registro. Y esta es una omisión grave.

3. *Necesarias distinciones acerca de las categorías de datos.*

La ley aprobada y el Acta del debate en Comisión Mixta distinguen distintos categorías de datos, sin un tratamiento sistemático en el cuerpo legal. Algunas, como veremos, se definen en el artículo segundo. Otros fueron mencionados en los respectivos debates parlamentarios. El concepto esencial y genérico es el de DATO PERSONAL, que es "el relativo a cualquier información concerniente a una **persona natural**, identificada o identificable". Revisten especial importancia los conceptos de datos personales "sensibles", personales "patrimoniales" o "económicos, financieros, bancarios o comerciales", pudiendo estos últimos ser positivos o negativos.

4. *Breves comentarios a las definiciones.*

El *artículo 2º* define 16 conceptos, no siendo las definiciones lo suficientemente claras.

[4] En un informe presentado al Senado en Mayo de 1998 reparamos esta iniciativa por inconstitucional. lo que fue acogido, según consta en las páginas 36 y 37 del informe final de la Comisión de Constitución, Legislación y Justicia del Senado.

Respecto de los datos se define cuando son "caducos"[5], "estadísticos"[6], "de carácter personal"[7] o personal "sensible"[8].

Respecto de las actividades de que pueden ser objeto los datos personales, el término más amplio que se define es "tratamiento de datos"[9], y derivados de este, los conceptos de "almacenamiento"[10], "bloqueo"[11], "comunicación o transmisión"[12], "eliminación o cancelación"[13], "modificación"[14] y "procedimiento de disociación"[15].

- [5] Conforme lo establece la letra d) del artículo 2°, "dato caduco" es el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición 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.

- [6] Letra e): ...dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

- [7] Letra f): ...datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

- [8] Son 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 la vida sexual.

- [9] 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.

- [10] Se entiende por tal a conservación o custodia de datos en un registro o banco de datos.

- [11] Consiste en la suspensión temporal de cualquier operación de tratamiento de los datos almacenados

- [12] La Comunicación o transmisión de datos es dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

- [13] Es la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

- [14] Consiste en todo cambio en el contenido de los datos almacenados en registros o bancos de datos

- [15] Se entiende por tal a todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

En relación a lo que podemos denominar la infraestructura del procesamiento de datos personales, el artículo define, como veremos, lo que es un "registro o banco de datos", el "responsable del registro o banco de datos", el "titular de los datos" y los "organismos públicos".

4.1 *"Fuentes accesibles al público".*

Una novedad de la ley chilena es la incorporación en términos amplísimos, a diferencia de la Ley Española[16], del concepto de "fuentes accesibles al público" en la letra i) del artículo 2°, las que legalmente han sido transformadas en la regla general. Se definen amplia y ambiguamente como "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado (es decir permitido) ...a los solicitantes".

La consecuencia práctica de esta norma es que al ser los datos legalmente públicos, cualquiera puede procesarlos y comercializarlos, validándose definitivamente el lucrativo negocio de la venta de datos personales.

La primera cuestión a dilucidar es determinar cuáles son los registros *"de datos personales públicos o privados de acceso no restringido o reservado a los solicitantes"*, porque los que no detenten esta calidad, aquellos cuyo acceso sea permitido, constituirán fuentes accesibles al público. La Ley no hace una categorización. No creemos que se trate de una cuestión meramente de hecho, sino que dicha determinación sólo podrá hacerse por los órganos jurisdiccionales pero para casos concretos. No obstante, ya en Chile existen algunas fuentes de información que son de acceso restringido ya que existen leyes que previamente así lo han establecido al darle a los datos el carácter de

[16] El artículo 28 de la Ley Española ya anotada, regula las fuentes accesibles al público solamente con el objeto de establecer que de esta clase de registros o bancos de datos pueden obtenerse datos patrimoniales positivos, dejando fuera de su alcance a los demas datos, especialmente a los sensibles. En tal Ley y las normas complementarias dictadas por la Agencia de protección de Datos se entiende por "datos accesibles al público" aquellos que se encuentran a su disposición en forma general y no impedidos por cuelquier norma limitativa (por ejemplo, datos de censos, anuarios, repertorios de jurisprudencia, archivos de prensa, guías telefónicas, etc.).

reservados o confidenciales. Nos referimos a lo menos al secreto estadístico (IN), al secreto tributario, al secreto bancario o al secreto de la filiación política. Al existir tales normas, son de acceso restringido; si no existieran (que es la regla general) serían de acceso permitido o fuentes públicas.

En relación con los datos personales-patrimoniales sujetos a secreto o reserva bancaria, al decir del artículo 2° letra i) serían precisamente de acceso restringido o reservado a los solicitantes y de conocimiento exclusivo tanto de las entidades financieras como de los titulares de dichos datos. Con todo, recordemos que es necesario distinguir lo que es el "secreto" de la "reserva" bancaria.

El *artículo 4°* establece que determinadas especies de datos que provengan de fuentes accesibles al público excepcionalmente no requieren autorización de sus titulares para ser tratados, lo que será tratado más adelante en forma detallada.

El *artículo 5°* inciso quinto señala que no se establecen limitaciones para la transmisión vía redes de "datos personales accesibles al público en general".

El artículo 9° establece que los datos personales que provengan o se hayan recolectado de fuentes accesibles al público pueden usarse para fines diversos de aquellos con que fueron recolectados.

Cabe sentar la siguiente conclusión: en Chile todas las fuentes de datos personales serán de acceso público, no restringido o reservado a los solicitantes, salvo que una ley establezca expresamente lo contrario.

5. *Análisis del artículo 4º*[17].

Ubicada en el Título I sobre la utilización de datos personales, se trata de la norma más conflictiva y confusa, misma que, en nuestra opinión, es clave para entender que estamos frente a una normativa que apuntó a proteger y legalizar el negocio del procesamiento de datos personales desde la perspectiva de las empresas del ramo, más que a resguardar los derechos de los titulares a quienes aluden o a quienes se refieren los datos personales o nominativos.

5.1 *Regla general.*

El artículo sienta un principio general en materia de procesamiento de datos personales, el que, atendidas las excepciones que luego consagra, no es sino una mera "declaración de principios". Señala que el tratamiento de los datos personales sólo podrá efectuarse cuando esta ley u otras disposiciones legales lo autoricen, o cuando el titular consienta expresamente en ello.

[17] ***Artículo 4°.*** *El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.*

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito.

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Respecto a "la autorización" mediante la cual el titular de los datos personales consiente expresamente en "el tratamiento"[18], señalan los incisos segundo, tercero y cuarto que tanto su otorgamiento como su revocación deben constar por escrito, que la revocación se produce, aunque sin efecto retroactivo, y que la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y de su posible "comunicación" al público. Como nada se dice, creemos que tal autorización podrá ser otorgada antes o después de iniciado el procesamiento, con lo cual caeríamos en el ámbito (el uso de la expresión es nuestro) de la *"ratificación"*.

Fácil es concluir que se transformará en una amplia cláusula tipo, especialmente en los contratos de adhesión, aquello de que *"por el presente instrumento se autoriza desde ya a.."*[19].

5.2 *Excepciones.*

La norma consagra diversas excepciones en los incisos quinto y sexto, en relación a la autorización del titular requerida para el tratamiento de los datos. Establece que en determinados casos ***no requiere autorización el tratamiento de datos personales que provengan o que se recolecten de "fuentes accesibles al público" (que ya sabemos son, por definición, la regla general).***

[18] Recuérdese que la letra o) del artículo 2° define como "tratamiento de datos" a "*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*".

[19] Estas cláusulas no son ajenas al actual sistema financiero chileno. Así por ejemplo, en las Condiciones Generales de la solicitud de productos de una Financiera se señala que el solicitante faculta a la entidad *"para proporcionar a sus empresas relacionadas todos los datos referidos a mi individualización que he facilitado en la presente solciitud de crédito, tales como nombre y apellidos, estado civil, domicilio, profesión u oficio, Carnet de Identidad Nacional, Rut, y si fuera requerido para ello, lo faculto para informar a sus empresas relacionadas acerca de los depósitos y captaciones que mantengo y las obligaciones que he contratado...".*

Dichas situaciones de excepción son las siguientes:

a) *Cuando sean de carácter económico, financiero, bancario o comercial.*

Esta excepción debe ser analizada distinguiendo entre datos patrimoniales "positivos" y "negativos" y en relación, como veremos, con lo dispuesto en los *artículos 17º, 18º y 19º (Título III de la ley, únicamente referido a comunicación a terceros de datos personales patrimoniales negativos).*

En materia de datos patrimoniales "positivos", relacionados con los ingresos, ahorros, gastos e inversiones de las personas, esta excepción legal sumada a la amplía definición de fuentes de acceso público, se puede estimar que es inconstitucional, toda vez que vulnera al artículo 19 N°4 de la CPE.

Distinto es el caso de los "negativos" o protestos, los que, en atención al cuidado del orden público económico y a la luz del artículo 19 N°12 de la CPE, sí deben poder ser procesados -con ciertos límites- y obviamente sin el requisito de la autorización previa de sus titulares. En consideración a éstos, y junto con no requerirse autorización para su "tratamiento" (concepto amplio), *el artículo 17 se encarga más adelante de precisar cuáles son los que específicamente o en qué casos los datos sobre incumplimiento de obligaciones pueden ser "comunicados" (concepto específico y modalidad de tratamiento) a terceros.*

b) *Cuando se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento.*

La expresión "tales como" demuestra que se trata por ende de una enumeración sólo ejemplar o *"numerus apertus"*. El uso de la expresión se traduce en que será una cuestión de hecho que en definitiva determinarán los tribunales para cada caso concreto sometido a su decisión, definir si un dato personal o nominativo es o no de aquellos contenidos en listados relativos a una categoría de personas que pueden ser tratados -con la amplitud de operaciones que involucra el término- sin autorización de sus titulares.

c) *Cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.*

El *marketing* directo o telemercadeo es una de las formas de gestión empresarial más eficaces para promocionar productos y ofrecer servicios. Es de la esencia para esta actividad comercial contar con bases o bancos de datos personales o nominativos, lo más completas posibles y con el mayor cúmulo de antecedentes que puedan recopilarse y cruzarse, para elaborar así perfiles de comportamiento mediante técnicas de procesamiento computacional conocidas como *"Data Mining"* o "Minería de Datos". A mayor información, mejor será la estratificación y focalización del segmento al cual apuntará la campaña comercial o la venta de los productos.

Si bien es cierto que desde un punto de vista comercial aparece conveniente la relación directa entre una empresa y sus clientes, la posibilidad de decidir que dicha relación exista o no, le compete a los consumidores, los que pueden desear mantenerse al margen y resguardar la privacidad de sus datos personales para no ser invadidos con agresivas campañas comerciales o promocionales y recibir *e-mails*, cartas, folletos o llamados telefónicos, y así debiera garantizarse jurídicamente.

La ley aprobada, a diferencia de toda la legislación extranjera, legaliza con mínimas limitaciones el marketing directo. El artículo 4° en comento establece como amplia excepción y perentoriamente, que no se requiere autorización para el procesamiento de datos personales que provengan de fuentes públicas cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, lo que, sumado a las dos excepciones anteriores o perfilados con los datos a que ellas aluden, declara exento de autorización o control para el titular a un cúmulo demasiado grande de datos nominativos o personales[20].

[20] Difícil tarea tendrán los congresistas que impulsaron la ley para explicar en el futuro la razón de que frente a una actividad esencial para las empresas de marketing directo y que sólo persigue fines de lucro o comerciales, inconstitucionalmente optaron por impedir que los chilenos "autodeterminen", autoricen y controlen el uso de sus antecedentes. Del mismo modo, se ha permitido legalmente que AFP, ISAPRE, multitiendas, Universidades,

Particularmente grave es la no exigencia de autorización o consentimiento de los titulares de los datos para la actividad consistente en "tratar" (recopilar, procesar, almacenar, cruzar, comunicar, etc.) antecedentes personales económicos, comerciales, patrimoniales y financieros positivos -que no dan cuenta de insolvencia patrimonial o de protestos-, quizás los más relevantes para las empresas de marketing directo, ya que la naturaleza o el contenido de la información que administran o su cartera de clientes es su principal activo.

Este artículo está en abierta contradicción con lo que dispone el *artículo 3°* inciso segundo, a saber, que el titular de los datos personales (la persona natural a que se refieren) puede oponerse -en nuestra opinión sin expresar causa alguna- a su uso "con fines de publicidad". Habría que entender que el inciso quinto del artículo 4° prima por especialidad.

Por cierto, el *artículo 12°* de la ley establece que la eliminación o el bloqueo de los datos (garantías que derivan del derecho de acceso) puede hacerse cuando los datos personales se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. *El problema está en que será muy difícil que los titulares de los datos sepan quiénes están tratándolos para realizar marketing directo.*

d) Cuando el tratamiento de datos personales lo realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

6. *Datos personales, encuestas, estudios de mercado y publicidad.*

El *artículo 3°* establece que *"en toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública* ***u otros instrumentos semejantes"*** (aquí cabe todo), *"sin perjuicio de los demás*

Asociaciones Gremiales, órganos públicos, etc. puedan comercializar grandes cúmulos de información, siempre con la ignorancia y sin el consentimiento de los titulares y propietarios de los antecedentes que los individualizan.

derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas".

Consagra el inciso segundo un "Derecho de Oposición" que puede ejercerse sin expresión de causa, señalando perentoriamente que *"el titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión".* Respecto a una especial forma de publicidad, a saber, el *marketing* directo, ya señalamos que el tema es regulado por el *artículo 4°* y que no se exige autorización del titular para procesar datos personales con estos fines, con lo que a su respecto la ley no permitiría ejercer este derecho de oposición.

Este derecho, al decir de un autor francés, refuerza el principio de que los titulares de los datos personales que les conciernan poseen un derecho de propiedad de los mismos, lo que es obvio si se tiene presente que se trata de información referida a atributos de su personalidad.

7. La relevante figura del "responsable del registro o banco de datos personales".

La letra n) del *artículo 2°* señala que reviste tal calidad *"la persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal".*

El mismo artículo define lo que debe entenderse por "registro o banco de datos", a saber, *"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".*

El *artículo 5°* faculta al responsable para establecer un procedimiento automatizado de datos personales.

El *artículo 6°* señala que el responsable tiene la obligación de eliminar, modificar o bloquear datos personales sin necesidad de requerimiento del titular (léase "de oficio").

El *artículo 11°* establece que el responsable de los registros o bases de datos personales deberá cuidar de ellos con la debida diligencia. Obviamente agrega que lo hará "con posterioridad a su recolección" y que se hará responsable de los daños producidos. Entendemos, en consecuencia, que responde de la culpa leve.

El *artículo 12°* lo indica como la persona ante quien se ejerce el denominado *"Habeas Data"* o *"Derecho de Acceso"*.

El *artículo 16°* señala que su domicilio determina la competencia de los tribunales.

El artículo 17° faculta al responsable, en las condiciones que más adelante se verá, para comunicar a terceros los datos patrimoniales negativos.

Un comentario final respecto del responsable: atendido que la ley eliminó la obligación que los responsables queden anotados en un registro público, es factible que los titulares de los datos personales nunca sepan de la existencia del banco de datos o el origen de los datos y que los responsables actúen en total anonimato y carentes de toda fiscalización por la autoridad.

Es paradójico: en el Derecho Comparado la conducta consistente en actuar en el ámbito del procesamiento de datos personales sin haberse registrado y sin autorización previa se sanciona con fuertes multas, e incluso es constitutiva de delito.

8. *El "Habeas Data" o "Derecho de Acceso"*.

Esta garantía esencial de toda ley de protección de datos y las facultades que de ella derivan, mismas que por su importancia en varios países tienen rango constitucional, están reguladas en los *artículos 12°, 13°, 14°* y *15°* de la ley, que son los primeros del Título II sobre "Derechos de los

titulares de datos", y se ejercen precisamente ante quien aparezca como responsable del registro.

En síntesis, la ley establece inicialmente que toda persona tiene derecho a exigir -a quien sea responsable de un registro banco de datos que se dedique en forma pública o privada al tratamiento de datos personales-, 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 regularmente.

De esta declaración inicial del derecho de *"acceder a la información"*, se derivan una serie de garantías o de facultades correlativas.

La *"modificación"* de los datos personales procede cuando sean erróneos, inexactos, equívocos o incompletos, y así se acredite.

La *"eliminación"*, salvo las excepciones legales, puede exigirse, en caso que el almacenamiento de datos personales carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de *"bloqueo de los datos"*, puede hacerse cuando se hayan proporcionado voluntariamente los datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Estas facultades no pueden ser cobradas por el responsable del registro, toda vez que se señala expresamente que las solicitudes de información, modificación o eliminación de los datos serán *"absolutamente gratuitas"*, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Del mismo modo son *"irrenunciables"*, por cuanto la ley señala que el derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

Para el evento que los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la

brevedad posible la operación efectuada; y si no fuese posible determinar las personas a quienes se les hayan comunicado, deberá publicarse un aviso que pueda ser de general conocimiento para quienes usen la información.

9. *Regulación de los datos sensibles "o personalísimos".*

Recordemos que el *artículo 2°* letra g) señala que son 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 la vida sexual.

El uso de la expresión "tales como" se traduce en que se trata de una cuestión de hecho que en definitiva determinarán los tribunales el definir si un dato personal o nominativo es o no sensible.

Ahora, el artículo 10° establece perentoriamente que "no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos de salud necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares".

10. *Comunicación a terceros de datos patrimoniales negativos (protestos y morosidad comercial).*

Entramos al ámbito del Título III de la ley, acerca de "la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", conformado por los *artículos 17°, 18° y 19°.*

El *artículo 17°* establece que los datos patrimoniales negativos que pueden "comunicarse" (transmitirse o darse a conocer de cualquier forma a terceros) por el responsable del registro o banco de datos, sin la necesidad de

autorización por escrito previa o ratificación posterior del titular[21], serán los que consistan en "información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial" incumplidas, exclusivamente en los siguientes casos[22]-[23]:

- Cuando las obligaciones incumplidas consten en letras de cambio y pagarés protestados";

- Cuando las obligaciones incumplidas consten en "cheques protestados por falta de fondos", cuando consten en cheques "que hayan sido girados contra cuenta corriente cerrada o por otra causa". (En consecuencia, no se encuentra limitado a cheques que estén protestados);

- Den cuenta (los datos) del incumplimiento de obligaciones derivadas de mutuos hipotecarios, y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación

▪ [21] Respecto a "la autorización" mediante la cual el titular de los datos personales consiente expresamente en "el tratamiento", señalan los incisos segundo, tercero y cuarto del artículo 4° que tanto su otorgamiento como su revocación deben constar por escrito, que la revocación se produce "aunque sin efecto retroactivo", y que la persona que autoriza debe ser debidamente informada por el responsable respecto del propósito del almacenamiento de sus datos personales y de su posible "comunicación" al público.

▪ [22] Por cierto, las hipótesis consideradas son todos ejemplos de incumplimiento de obligaciones.

▪ [23] El inciso primero señala literalmente: "L*os 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 falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios, y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.*

común, *y de sociedades administradoras de créditos otorgados para compras en casas comerciales*[24].

Datos relacionados con aquellas otras obligaciones de dinero que determine el Presidente de la República mediante Decreto Supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento.

- En nuestra opinión, cabe agregar un quinto caso de comunicación de datos patrimoniales negativos a terceros, amplio, que serían todas aquellas hipótesis en que en virtud del principio general del *artículo 4º* los titulares de los datos autoricen o consientan expresamente en el tratamiento, por escrito y habiendo sido debidamente informados respecto del propósito del almacenamiento de sus datos personales y de su posible "comunicación" al público.

Del análisis del Acta del debate de la Comisión Mixta (páginas 45 y ss.), elemento clave para interpretar el alcance del artículo 17°, así como la historia fidedigna del establecimiento de la ley, claramente se concluye que esta norma restrictiva sólo alude a los datos patrimoniales negativos y al incumplimiento de obligaciones económicas, comerciales, bancarias y financieras.

Cabe concluir que el *artículo 17º* no alude a los datos patrimoniales de carácter económico, financiero, bancario o comercial "positivos" o no fundados en el incumplimiento de una obligación, los que sí pueden "tratarse" ampliamente (recopilarse, procesarse, almacenarse, comunicarse, cruzarse, etcétera) en conformidad a lo que dispone el *artículo 4º*, esto es, sin autorización del titular de los datos en la medida que provengan de fuentes

[24] Esta frase fue agregada durante el debate en Comisión Mixta a instancias de la Cámara de Comercio de Santiago.

accesibles al público. Los parlamentarios nunca tuvieron la intención de excluir la posibilidad de que los datos patrimoniales positivos sean comunicados o suministrados a terceros, alcance que de todas maneras habría sido consignado en el Acta o Informe Final, sino que incluso contemplaron la posibilidad "excepcional" (así entre comillas) de hacerlo sin autorización de sus titulares.

El *artículo 18°* es la norma que apunta a poner término a los denominados *"Archivos Históricos"*. A estos efectos, establece que las empresas o entidades que presten servicios de solvencia patrimonial (no los acreedores por si mismos) en ningún caso pueden comunicar los datos patrimoniales negativos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos ***siete años*** desde que la respectiva obligación se hizo exigible, y que tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos ***tres años*** del pago o de su extinción por otro modo legal.

La excepción está dada, obviamente, porque se podrá comunicar a los tribunales de justicia la información o los datos personales que ellos requieran con motivo de juicios pendientes.

El *artículo 19°*, por último, sienta como principio general que son compatibles el ejercicio del derecho de acceso contra el responsable de un banco de datos con información patrimonial negativa con el hecho de haberse pagado o extinguido las obligaciones de que ellos dan cuenta, y extrae una serie de consecuencias al efecto.

11. *Aspectos procesales.*

Se trata ahora de poner en práctica o hacer operar procesalmente el Derecho de Acceso consagrado en el *artículo 12°*.

Ante la inexistencia de un órgano administrativo ad hoc, la acción civil que contempla la ley en favor del titular de los datos personales se ejercerá directamente ante los tribunales ordinarios de primera instancia, cumpliéndose un presupuesto esencial, esto es, haber accionado previamente

ante el responsable para informarse, eliminar, cancelar o bloquear datos y que éste no haya respondido en el plazo de dos días.

> Al tema se refiere el *artículo 16°*, a cuyo contenido literal nos remitimos.

Bástenos dejar señalado que el intento de establecer un procedimiento breve y sumarísimo, tanto en primera como segunda instancia, no está a la altura de los procedimientos de reclamo administrativo que contemplan todas las leyes del Derecho Comparado.

Del mismo modo y por la importancia de los bienes jurídicos afectados (garantías constitucionales), creemos que al menos el conocimiento del *"Habeas Data"* en primera instancia debió habérsele encomendado a las Cortes de Apelaciones, de la misma manera que se ha hecho en Chile con el denominado Recurso de Protección.

Llama la atención que la norma señale que son improcedentes los recursos de casación. Esto significa que en materia de legislación tratamiento de datos personales no existirá la posibilidad de uniformarse la jurisprudencia, al no poder los tribunales conocer de aquellas infracciones de ley que hayan influido sustancialmente en lo dispositivo del fallo.

V. TEXTO DE LA LEY APROBADA POR EL CONGRESO NACIONAL

PROYECTO DE LEY:

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Título Preliminar
Disposiciones generales

Artículo 1°. *El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley.*

Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

Artículo 2°. *Para los efectos de esta ley se entenderá por:*

a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.

b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

d) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición 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.

e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

g) Datos sensibles, 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 la vida sexual.

h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

m) Registro o banco de datos, 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.

n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

o) Tratamiento de datos, 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.

Artículo *3°. En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas.*

El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

Título I
De la utilización de datos personales.

Artículo 4°. *El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.*

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito.

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Artículo 5°. *El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.*

Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:

a) La individualización del requirente;

b) El motivo y el propósito del requerimiento, y

c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

Artículo 6°. *Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.*

Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular.

Artículo 7°. Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con la base de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

Artículo 8°. En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales.

El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

Artículo 9°. 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.

En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

Artículo 10. No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos de salud necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Artículo 11. El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Título II
De los derechos de los titulares de datos

Artículo 12. *Toda persona tiene derecho a exigir a quien sea responsable de un banco que se dedique en forma pública o privada al tratamiento de datos personales, 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 regularmente.*

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan

comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

Artículo 13. *El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.*

Artículo 14. *Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos.*

Artículo 15. *No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.*

Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva.

Artículo 16. *Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de 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, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente.*

El procedimiento se sujetará a las reglas siguientes:

a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso.

b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario.

f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes.

h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en

un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma Sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública.

En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales.

La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere 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.

Título III
De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial.

Artículo 17. *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 falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios, y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas*

del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.

También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento.

Artículo 18.- *En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible.*

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos tres años del pago o de su extinción por otro modo legal.

Con todo, se comunicará a los tribunales de justicia la información que requieran con motivo de juicios pendientes.

Artículo 19.- *El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente.*

Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16.

Título IV
Del tratamiento de datos por los organismos públicos

***Artículo** 20. El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular.*

***Artículo** 21. Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.*

Exceptúase los casos en que esa información les sea solicitada por los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5°, 7°, 11 y 18.

***Artículo** 22. El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos.*

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación 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.

Título V
De la responsabilidad por las infracciones a esta ley

Artículo 23. *La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en caso, lo ordenado por el tribunal.*

La acción consiguiente podrá interponerse conjuntamente con la demanda destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

Título Final

Artículo 24. *Agrégase los siguientes incisos segundo y tercero, nuevos, 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 divulgue 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.".

Disposiciones transitorias

Artículo 1º. *Las disposiciones de esta ley, con excepción del artículo 22, entrarán en vigencia dentro del plazo de sesenta días, contados desde la fecha de su publicación en el Diario Oficial.*

Los actuales registros o bancos de datos personales de organismos públicos se ajustarán a las disposiciones de este cuerpo legal, a contar de su entrada en vigencia.

Lo dispuesto en el artículo 22 comenzará a regir un año después de la publicación de esta ley. Sin perjuicio de lo anterior, los organismos públicos que tuvieren a su cargo bancos de datos personales deberán remitir los antecedentes a que se refiere dicho precepto con anterioridad, dentro del plazo que fije el reglamento.

Artículo 2°. *Los titulares de los datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de la presente ley tendrán los derechos que ésta les confiere.*

Artículo 3º. *Las normas que regulan el Boletín de Informaciones Comerciales creado por el Decreto Supremo de Hacienda Nº 950, de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley.*

Acordado en sesiones celebradas los días 16 de diciembre de 1998, 5 y 19 de enero, 13 y 20 de abril de 1999 con la asistencia de los HH. Senadores señores Hernán Larraín Fernández (Presidente), Jorge Martínez Bush, Juan Hamilton Depassier, José Antonio Viera-Gallo Quesney, Enrique Zurita Camps y de los HH. Diputados señores Alberto Cardemil Herrera, Juan Antonio Coloma Correa (Francisco Bartolucci Jonston y Julio Dittborn Cordúa), Sergio Elgueta Barrientos, Eugenio Tuma Zedán y Zarko Luksic Sandoval.