MODELO DE PROPUESTA REGULATORIA AL MERCADO DE DATOS PERSONALES EN CHILE

Paula Jervis Ortiz

Magíster en Derecho y Diplomada en Derecho Informático
por la Universidad de Chile. Investigadora del Centro de Estudios
en Derecho Informático de la Facultad de Derecho de la Universidad de Chile.

RESUMEN

La autora propone una reforma al modelo de protección de datos de Chile en base a criterios de propietarización vinculados a la diversa naturaleza de los datos de las personas, lo que da oportunidad a establecer modalidades contractuales de protección de derechos fundamentales.

PALABRAS CLAVE

Derecho de propiedad, protección de datos personales, autonomía de la voluntad, contratación modelos de regulación.

ABSTRACT

The author proposes a reform to the model of data protection of Chile on the criteria basis of proprietorship linked to the diverse nature of the people data, which gives opportunity to establish contractual modalities of protection of fundamental rights.

KEY WORDS

Property right, personal data protection, autonomy of the will, hiring, regulation models

1.- INTRODUCCIÓN

En prácticamente todas las sociedades el control y acceso a la información se han convertido en instrumentos de poder para el que la posee, sobre todo desde que ésta puede ser comprada, vendida o canjeada por aquellos que reconocen su valor[1]. Como indica Keneth Laudon[2]. "Todos los días profesionales capacitados compran y venden enormes cantidades de información sobre millones de individuos en forma de listas de correo, archivos de información computacional, información demográfica, e información sobre situaciones determinadas. Nosotros sabemos que

1 WELLS, Anne. 1994. Who owns information. New York, Basic Books. 241p.

2 LAUDON, Keneth. Extensions to the theory of markets and privacy: mechanics of pricing information. [en línea] <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1D> [consulta: 11 febrero 2005] Pág. 4.

los gobiernos, las instituciones de crédito, las compañías de seguros, las agencias de reportes de crédito son los mayores compradores de información personal. Sabemos también que este comercio de información personal involucra billones de dólares. Y todavía no sabemos el tamaño total de este comercio, cómo los comerciantes deciden los precios de compra y de venta, o incluso, cuánto vale el registro de conductor, el registro de seguro médico o registros de créditos."

Tanto los titulares de datos como aquellos que efectúan tratamiento de ellos, asignan valor al control que puedan ejercer sobre la información personal. Así, encontramos dos tipos de conductas referidas a los datos personales, según sea el sujeto que se relaciona con ellos: es posible de una parte que los titulares de datos no deseen que su información personal sea tratada, y de otra, es posible encontrar a alguien que desee procesar tal información para una multiplicidad de fines, por ejemplo, para efectuar marketing directo[3]. Lo descrito anteriormente genera un claro conflicto de intereses entre dos sujetos[4], conflicto que en algún momento debe ser dirimido por algún método, ya sea la autorregulación por parte de quienes quieren efectuar el tratamiento de datos personales por medio de códigos deontológicos o códigos de conducta; mediante normas legales que asignen las titularidades correspondientes y las formas de protección de ellas; por acuerdo entre las partes; por el mercado o, finalmente, utilizando en forma conjunta algunas de las vías mencionadas anteriormente. Uno de los objetos de este trabajo es referirse a estos distintos métodos y descubrir cuáles de ellos nos pueden llevar a una solución eficiente en términos económicos, para ello, en primer lugar se efectúa una revisión de las críticas realizadas a la Ley 19.628 sobre Protección a la Vida Privada, luego se revisan los diversos modelos de protección de datos personales que hemos encontrado en la doctrina. Finalmente, se elabora un modelo de protección denominado modelo de autonomía y que está compuesto de los siguientes elementos: i) Propietarización; ii) Contratos; iii) Asignación de derechos y reglas de protección; iv) Control del titular de los datos personales; v) Responsabilidad y régimen sancionatorio. Por último, hacemos una referencia a las críticas doctrinarias que podrían aplicar al modelo planteado.

2.- CRÍTICAS EFECTUADAS AL MODELO REGULATORIO CHILENO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La Ley 19.628 que regula la protección de la vida privada en Chile, ha sido duramente criticada casi desde su entrada en vigencia, estableciéndose respecto de ella, ciertos vacíos e inconsistencias. Prueba de ello, son los múltiples proyectos de ley que se han presentado con el

[3] Jerry KANG, 1998. *Information privacy in cyberspace transactions*. Stanford Law Review 50: 1193-1294. pág. 1246.

[4] A este respecto es muy interesante lo señalado por Jerry KANG, sobre los fundamentos que esgrimen los que efectúan tratamiento de datos personales para que la balanza se incline a su favor, quienes señalan, según este autor, que la información personal es generada en una mutua interacción, en la cual ambas partes son participantes, entonces, ¿porqué se debería preferir los derechos de los titulares de datos sobre lo que fue producido conjuntamente? Creemos que este fundamento es aplicable sólo a aquellos tratamientos que impliquen de alguna u otra manera esta interacción entre las partes involucradas, como por ejemplo, cuando son partes de una relación contractual, cuando la interacción se genera en Internet, pero no se puede aplicar en casos en que el tratamiento de datos se efectúa sin ninguna intervención del titular de ellos. Jerry KANG, Ibídem. De su parte, Anne WELLS indica que existen dos grupos de conflicto a propósito de la información personal: En el primero de ellos, una de las partes alega que nadie es dueño de la información, de manera que la información es propiedad pública demasiado importante para el bienestar de la sociedad para que cualquier empresa comercial tenga el poder de restringir su uso o disponibilidad. En el segundo, un argumento muy diferente es expuesto: la comercialización de la información está en conflicto con las nociones establecidas acerca del derecho de los individuos a la privacidad sobre cierta información personal. Anne WELLS. op.cit. pág. 3.

objeto de modificar la normativa vigente y que se encuentran actualmente en tramitación en el Congreso Nacional[5].

Rodolfo Herrera entrega una suerte de catálogo de críticas a la ley 19.628, que pasamos a sistematizar a continuación:

- La protección de la vida privada –que orientó desde sus orígenes la discusiones parlamentarias y a la que alude incluso la denominación de la Ley- cede, a veces en exceso, ante los derechos del responsable del registro, a causa de la insuficiencia de algunas garantías.
- Contiene demasiadas disposiciones especiales para ciertos datos contenidos en fuentes accesibles al público que quitan terreno a las normas generales de protección ordinaria.
- No existe un órgano de control encargado de velar por el cumplimiento de la Ley.
- No se contempla un derecho al recurso -por vía administrativa, civil o, incluso, penal-, con sanciones y responsabilidades para quienes incumplan las disposiciones legales.
- Inexistencia de la obligación de registro de los bancos de datos privados.
- Otras omisiones graves, por ejemplo, en materia de seguridad, en la necesidad de consentimiento del titular para realizar las comunicaciones a terceros o en relación con la transferencia internacional de datos.

[5] Boletín 3382-15 "Moción que resguarda el derecho a la vida privada en materia telefónica".

Boletín 2422-07 "Establece normas sobre protección de la información de las personas jurídicas".

Boletín 2474-07 "Amplía beneficios de la ley sobre protección a la vida privada, en lo relativo a informes comerciales, a las personas jurídicas comprendidas en el artículo 545 del Código Civil".

Boletín 2600-18 "Establece la comunicación al Boletín Comercial de los incumplimientos graves de deudas alimenticias".

Boletín 3003-19 "Establece la privacidad de los datos recolectados a través de Internet".

Boletín 3185-19 "Modifica ley sobre protección de datos personales estableciendo normas sobre el uso de bases de datos en los correos electrónicos".

Boletín 3796-07 "Modifica la ley Nº 19.628, sobre protección de la vida privada, con el fin de evitar el uso abusivo de datos personales o de empresas y de resguardar a los usuarios de correos electrónicos de la propaganda comercial no solicitada".

Boletín 4203-07 "Modifica la ley Nº 19.628, respecto de la obligación del deudor de pagar los costos de información del pago de la deuda."

Boletín 4429-07 "Modifica la ley Nº 19.628, sobre protección de la vida privada, con el objeto de resguardar en mejor forma los datos de carácter personal y sancionar penalmente su tratamiento y cesión indebida."

Boletín 4436-03 "Modifica la ley Nº 19.628, suspendiendo por un plazo determinado la información comercial de las personas cesantes."

Boletín 4466-03 "Modifica la ley Nº 19.628, con el objeto de ampliar los mecanismos de protección de los datos de carácter personal."

Boletín 4159-03 "Deroga el decreto supremo Nº 950, del Ministerio de Hacienda, de 1928, sobre boletín comercial."

Para este autor, "lejos de tratarse de críticas meramente formales o de segundo orden, son errores esenciales del legislador que reafirman nuestra opinión sobre la Ley N° 19.628, y nos llevan a concluir que en Chile aún está pendiente el tema de la protección de datos personales"[6].

Otro autor nacional, Francisco GONZÁLEZ HOCH[7], plantea la necesidad de reforma de la Ley 19.628, por cuatro razones:

- Inexistencia de un órgano de control, que obliga a los particulares a recurrir a los Tribunales de Justicia, lo que significa necesariamente alto costo para las víctimas.
- Dificultades de la responsabilidad por culpa, que pone de cargo de la víctima la carga onerosa y prácticamente imposible de acreditar culpa o negligencia.
- Inexistencia de un registro de bases de datos privadas, lo que dificulta el ejercicio de los derechos, especialmente a personas naturales.
- Multas que no significan disuasivos reales, el establecimiento de multas de monto relativamente reducido en comparación con el patrimonio de las administradoras de bases de datos y su volumen de negocios no establece incentivos suficientemente fuertes para cumplir la ley.

Alberto Cerda también efectúa críticas a la ley en comento, indicando que "La extensión de sus hipótesis de excepción, ciertas ambigüedades de su texto y la carencia de disposición alguna que prevea mecanismos de control ante el tratamiento ilegítimo de datos personales, entre otras falencias, permiten afirmar que más que una normativa que tiene por objeto velar por los derechos de los afectados por el tratamiento de datos constituye el marco jurídico al cual se afecta tal tratamiento, lo cual queda, por lo demás, avalado constantemente de la historia fidedigna de su establecimiento, en la cual se consigna el afán de resguardar la actividad desplegada por los prestadores de servicios de información y entidades tratantes de datos en general"[8].

De nuestra parte, compartimos algunos de los reparos efectuados a la Ley 19.628 por la doctrina nacional, agregando algunos, así concluimos que:

- La ley referida no propende a un equilibrio entre la información que poseen los actores en el tratamiento de datos personales, ya que sólo existe un registro de datos públicos, y éste ni siquiera es completo, lo que lleva a que los titulares de los datos personales desconozcan quién trata su información personal y cómo lo hace.
- El titular de los datos no participa en ninguna de las etapas del proceso de comunicación de sus datos a terceros distintos del responsable del registro (mercado secundario), lo que aumenta la asimetría de información.

[6] Rodolfo HERRERA. Privacidad e Internet: El problema del tratamiento invisible y automatizado de datos personales. [en línea] <http://www.adi.cl/documents/01invis.pdf> [consulta: 29 marzo 2005]. Nota 10 pie de página.

[7] Francisco GONZÁLEZ HOCH, 2001. Modelos comparados de protección a la información digital y la ley chilena de datos de carácter personal. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 153-178. pág. 177.

[8] Alberto CERDA SILVA. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. (Magíster en Derecho). Santiago, Chile. Facultad de Derecho Universidad de Chile. 2003. 260h. pág. 97. Otros autores han criticado la normativa vigente en Chile con similares argumentos. V. a. Renato JIJENA, "Sobre la no protección de la intimidad en Chile. Análisis de la ley 19.628, de agosto de 1999". [en línea] <http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Sobre-no-proteccion-intimidad-Chile-Analisis-Ley-19-628-Agosto-1999/2100-115523,01.html> [consulta: 19 marzo 2006]; MAGLIONA, Claudio. "Breve análisis de la ley número 19.629 sobre protección a la vida privada". [en línea] http://www.alfa-redi.org/rdi-articulo.shtml?x=592 [consulta: 19 marzo 2006].

- No existe un reconocimiento que valide a los códigos deontológicos o de conducta como complemento de la legislación sobre protección de datos personales.
- No existe regulación respecto de la transferencia transfronteriza de datos, lo que hace que nuestro país no cumpla en esta parte con los estándares internacionales y se dificulte este tipo de transferencias, como asimismo, que nuevamente los titulares de la información que se transfiere tengan poco o nada que decir al respecto.
- El régimen sancionatorio que establece penas irrisorias frente a infracciones a la norma no incentiva su cumplimiento.
- Se debiera incluir a las personas jurídicas como sujetos de protección de la norma ya que no se logra vislumbrar desde un punto de vista práctico y económico el porqué sólo se protege a las personas naturales.
- Se mantiene una suerte de monopolio legal a favor de la Cámara de Comercio de Santiago respecto de los datos patrimoniales.
- Asimismo, podemos afirmar sin temor a equivocarnos que la ley es poco clara y contradictoria en algunos de sus articulados.
- Finalmente, creemos que la asignación de titularidades que se ha efectuado en la norma en algunos casos es errada.

Todos los puntos expuestos anteriormente nos llevan a concluir que estamos en presencia de una norma legal que es ineficiente tanto desde un punto de vista económico, como asimismo, desde la finalidad declarada por la ley, cual es proteger a los titulares de datos personales.

Dado lo anterior, intentaremos teorizar respecto de un nuevo modelo de protección de datos personales en nuestro país. A estos efectos revisaremos, en primer lugar, qué modelos de protección se han planteado por la doctrina extranjera.

3.- ALGUNOS MODELOS DE PROTECCIÓN DE DATOS PERSONALES

A continuación revisaremos cinco modelos de protección a la privacidad informacional desarrollados por algunos de los autores consultados a efectos de esta tesis. Se escogieron estos cinco modelos, ya que cada uno de ellos representa las posturas mayoritarias que en esta materia hemos encontrado.

3.1.- MODELO TRADICIONAL DE PROTECCIÓN

Julie COHEN[9], que tiene una mirada conservadora y bastante europea de lo que debe ser un modelo de protección de datos personales, señala que éste debe estar constituido por una fuerte legislación protectora de datos que cree y preserve una zona de autonomía informacional para los individuos. Este modelo, en base a lo anterior, debe cumplir con tres requisitos:

a) Debe encontrar un equilibrio entre la propiedad y la libertad de expresión.[10]

[9] Julie COHEN. 2000. Examined Lives: Informational privacy and the subject as object. Stanford Law Review 52: 1373-1437. pág. 1428.

[10] Desde nuestro punto de vista, es decir, el nacional, este modelo debiera no sólo encontrar un equilibrio entre la protección de la privacidad de los titulares de datos personales y la libertad de expresión de los que efectúan tratamiento de datos, sino que también entre otros bienes jurídicos involucrados como el derechos de propiedad, libre desarrollo de actividad económica, derecho a la propiedad, entre otros.

b) Debe definir los parámetros adecuados en que los titulares de datos pueden escoger acerca de las prácticas de privacidad, con el objeto de asegurar que el consentimiento en la recolección, uso e intercambio de datos personales, sea informado y efectivo. Para esta autora, el titular de los datos debe poder consentir o rehusar la utilización de su información personal en cada segundo uso o transferencia. Agrega a lo anterior, que el consentimiento debe expirar después de un determinado lapso de tiempo, debido a que es muy difícil de prever los distintos tipos de usos de que pueden ser objeto los datos personales a largo plazo, de manera que pasado un lapso de tiempo, se debe requerir un nuevo consentimiento. Por último, indica, estas reglas mínimas para el consentimiento no serán efectivas, si el que ha recabado el consentimiento puede transferir el dato personal a terceros sin las restricciones iniciales establecidas para el uso del dato.

c) Debe incorporar protecciones adicionales que mantengan a la industria procesadora de datos responsable frente a los individuos y a la sociedad dentro de la que opera. Lo anterior, a través de la incorporación de ciertos principios que deben informar el actuar de los titulares de bancos de datos. En particular, estos principios deben establecer la transparencia de las prácticas de tratamiento de datos, la seguridad en el tratamiento, acceso al titular de los datos y la oportunidad de corregir inexactitudes, y la responsabilidad de quienes efectúan tratamiento de datos.

Agrega esta autora[11] que respecto de ciertos datos que requieren ser intercambiados para que funcione una determinada industria, como por ejemplo: reportes de crédito, investigación biomédica y de salud, servicios financieros y de seguros, las legislaciones protectoras de datos deben incluir reglas especiales, y especificar los tipos de datos a los cuales se les aplican estas reglas especiales, señalando además los principios de uso justo de la información que deben gobernar a las industrias que tratan este tipo de datos.

3.2.- MODELO DE PROPIETARIZACIÓN EN BASE A UNA INALIENABILIDAD HÍBRIDA

Paul Schwartz[12] construye un modelo de propietarización de los datos personales que implica el desarrollo de una inalienabilidad híbrida que consiste en la aplicación de restricciones al uso y transferencia de información personal más una regla de *opt-in*[13]. Este régimen permite una inicial transferencia de datos personales desde el titular de ellos, pero sólo si este titular tiene garantizada una oportunidad de bloquear futuras transferencias o usos por entidades no afiliadas o autorizadas.

Para este autor el modelo debe necesariamente contar con los siguientes elementos: Inalienabilidades, normas legales supletorias, derecho a salida, daños e instituciones. Analizaremos brevemente cada una de ellas.

a) Inalienabilidad: Según este autor la propietarización de los datos personales requiere de la creación de inalienabilidades para responder a los problemas de fallas del mercado[14] y

[11] Cohen, op. cit. pág. 1430.

[12] Paul Schwartz. 2004. *Property, privacy, and personal data*. Harvard Law Review. 117: 2056-2128. pág. 2060.

[13] Bajo una regla de "*opt-in*", un individuo debe dar su autorización previa para que sea legítimo el tratamiento de datos. Bajo una regla "*opt-out*" el titular de banco de datos tiene el derecho a tratarlos a menos que el titular de datos respectivo solicite que no sea utilizado. Los partidarios de la privacidad están generalmente a favor de *opt-in*; en este sentido, ellos creen que esa información no se debe utilizar a menos que el titular de los datos permita específicamente este uso.

[14] Señala Paul Schwartz que la libre alienabilidad es problemática debido a la asimetría de información existente en el tratamiento de datos y las políticas de privacidad, problema que se acentúa en el caso de

responder a la necesidad de obtener privacidad informacional[15]. Estas inalienabilidades estarían constituidas por la restricción en el uso de los datos personales y una limitación a su transferibilidad, "en la práctica este modelo permitiría la transferencia de una categoría inicial de uso de los datos personales, pero sólo si el titular de los datos tiene la garantía de bloquear futuras transferencias o usos a entidades no afiliadas (no autorizadas). Cualquier uso o transferencia futura, requerirá la autorización del titular de la información personal"[16]; este modelo constituiría un incentivo para el que efectúa tratamiento de datos en orden a suministrar información adicional al titular de los datos, si es que desea utilizar o transferir su información personal de una manera no autorizada previamente, negociando con el titular de los datos una nueva autorización.

c) Normas legales supletorias: Paul Schwartz establece el uso de normas legales supletorias *(defaults)* como una manera más de salvaguardar la elección individual del titular de los datos. Se muestra partidario de una regla opt-in, porque puede forzar la información, es decir, puede poner presión en la parte mejor informada para que revele información sobre cómo los datos personales serán usados. Lo anterior promete forzar la revelación de información oculta sobre las prácticas de procesamiento de datos. Paul Schwartz aboga porque este *default* sea obligatorio, esto es, que la ley prohíba a las partes negociar fuera de una regla de *opt-in*.

d) Derecho de salida: El modelo no sólo debe implicar una oportunidad inicial de consentir en el tratamiento de los datos por parte de su titular, sino también debe permitirle la posterior opción de dejar sin efecto la autorización. Este derecho de salida previene que malas negociaciones iniciales tengan un efecto a largo plazo.

e) Daños: El cuarto elemento que menciona Paul Schwartz es el establecimiento y la determinación del monto de los perjuicios que se puedan provocar por el tratamiento de datos en la legislación protectora de datos personales. Lo anterior, debido a que para este autor, el establecimiento de este tipo de daños ayuda a la operación del mercado de datos personales y a la construcción y mantenimiento de la privacidad informacional, ya que incentiva a las empresas a mantener sus promesas de privacidad a través del establecimiento de perjuicios lo suficientemente altos que evitan potenciales violaciones y fomenta la interposición de acciones que tengan por objeto defender las asignaciones en materia de privacidad.

f) Instituciones: Por último, para este autor el modelo necesita instituciones descentralizadas que cumplan una triple función, a saber: que provean mecanismos de mercado (*market-making function*), que verifiquen las demandas por datos personales (*verification function*) y que vigilen la conformidad de los acuerdos sobre transacción de datos personales con las obligaciones legalmente establecidas a este respecto (*oversight function*). Las instituciones que cumplan con estas funciones ayudarán al mercado de datos personales asegurando

los usos secundarios o múltiples de datos personales. La situación descrita, produce una real limitación para el establecimiento de un modelo de mercado de datos, ya que los titulares de la información personal no tienen la posibilidad de negociar los futuros usos de su información (debido a la existencia de la asimetría de información). Para mitigar este efecto negativo, este autor propone limitar tanto el uso como la transferencia de datos personales. Schwartz, op. cit., pág. 2097.

[15] Indica este autor, que el mercado causará que la gente venda su información personal o la intercambie por servicios adicionales o un menor precio en productos, pero no necesariamente fomentará la coordinación entre los deseos individuales de privacidad y la creación de privacidad informacional. Por lo anterior, es que fundamenta el establecimiento de ciertas limitaciones al uso y a la transferencia de datos personales. Schwartz, op. cit. pág. 2098.

[16] Schwartz, op. cit. pág. 2098.

que existan procesos para el intercambio de datos y para la detección de violaciones a la privacidad informacional.

3.3.- MODELO BASADO EN LA DISTINTA NATURALEZA DE LOS DATOS PERSONALES

Stan KARAS[17] también intenta un nuevo modelo de protección de datos personales, "que incorpore tanto el significado cultural del tratamiento de datos como los principios básicos de la legislación sobre privacidad", especialmente ideado para el ámbito de los consumidores en tanto titulares de información personal. Para este autor, en orden a apreciar la amenaza a la privacidad, es necesario determinar el tipo de información que es recolectada y cómo ésta es usada. Señala que se debe distinguir entre la información que es expresiva de la identidad[18] de una persona de aquella que no lo es, denominando a la primera "información expresiva", la cual considera privada y, por lo tanto, susceptible de ser protegida, mientras que aquella que no presenta estas características debiera encontrarse fuera de la protección legal a la privacidad. En el ámbito del tratamiento de datos de consumidores, la premisa anterior implica que sólo se deben proteger los datos personales que expresen la identidad de los individuos en tanto consumidores. Por último, este autor indica, respecto a la forma en que debe ser usada la información personal para que ésta sea protegida, que la privacidad sea amenazada, y consecuentemente debe ser amparada, cuando los datos personales son compilados en archivos o registros que revelan la identidad personal del individuo en tanto consumidor.

3.4.- MODELO CONTROL INDIVIDUAL

La organización sin fines de lucro norteamericana PrivacyRight, elaboró un *whitepaper* que contiene ideas muy interesantes respecto a los modelos de privacidad informacional, distinguiendo entre el control individual y el control organizacional.

Así, se indica que desde que los que efectúan tratamiento de datos son propietarios de los datos que recolectan, tienen incentivos para usar la información en formas que resultan inconsistentes con el propósito por el cual los datos fueron recolectados. Las consecuencias para los titulares de datos en un modelo como el de "control organizacional" incluyen marketing no solicitado, la propagación de información incorrecta, robos de identidad, y todo tipo de daños colaterales como la imposibilidad de obtener empleo o seguros debido a información incorrecta. Las empresas sufren daños económicos debido a demandas, pérdidas de clientes y deficiencias relacionadas con información incorrecta. Ante esta situación muchos creen que la única solución a estas fallas de mercado es la regulación del Estado. Sin embargo, un análisis económico cuidadoso puede sugerir que no lo es. Se señala, aplicando Coase, que la clave es asignar la propiedad de los datos personales a quien pueda resolver los problemas de privacidad como, por ejemplo, la integridad de los datos, riesgos de litigación, y molestia de los consumidores de la manera más eficiente. En la década de los 70, cuando los recursos computacionales eran escasos y extremadamente caros, el modelo de control organizacional hacía mucho sentido. Sólo grandes empresas tenían el capital necesario para comprar y mantener costosos sistemas de bases de datos personales y asumir el alto costo de garantizar acceso a los titulares de datos a los referidos sistemas. En este ambiente, el modelo de control organizacional funcionaba porque las empresas eran las únicas partes que podían manejar los datos personales eficientemente. En nuestros días,

[17] Stan KARAS, 2002. *Privacy, identity, databases: Toward a new conception of the consumer privacy discourse*. Stanford Technology Law Review. [en línea] <http://stlr.stanford.edu/STLR/Working_Papers/02_Karas_1> [consulta: 12 febrero 2005]. pág. 110.

[18] Stan KARAS entiende por identidad cualquier información que pueda distinguir a un individuo.

los recursos computacionales ya no son ni caros ni escasos. Los datos personales son comunicados entre diez o más bancos de datos dentro de una empresa, y éstas usualmente intercambian la información con terceras partes. Este intercambio puede añadir valor a la empresa, pero también puede aumentar el riesgo, que la información personal pierda actualidad o integridad, o sea mal usada después de su venta. Para manejar estos riesgos, las empresas debieran considerar un nuevo modelo de intercambio de información personal en donde se incorpore a los individuos que están en mejores condiciones de asegurar la integridad de la información. Este modelo, el de "control individual", debe ser implementado y debe permitir a los titulares de datos acceder y controlar apropiadamente a los bancos de datos y proveer la posibilidad de autorizar a través de comunicaciones electrónicas el uso de los datos personales a las empresas. Este cambio de modelo aumenta la integridad de la información personal recolectada, aumenta la confianza del titular de los datos y reduce los riesgos que en razón de la privacidad puede tener la empresa. Se producen grandes beneficios a un muy bajo costo. Así, mientras los defensores de la privacidad proponen entregar a los titulares de datos derechos de propiedad sobre sus datos personales por motivos ideológicos, el modelo de Coase muestra que hay fundamentos económicos para ello. Finalmente, se reconoce que en todo caso, hay situaciones en que dar a los titulares de datos control absoluto sobre su información personal puede no ser apropiado, por ejemplo, ciertos datos relacionados con el historial crediticio u otra información financiera[19].

3.5.- MODELO MERCADO NACIONAL DE INFORMACIÓN

Keneth LAUDON[20] establece un muy innovador e interesante modelo basado en un mercado nacional de información: señala la posibilidad de que los distintos datos personales de un individuo sean clasificados y puestos en un mercado público al cual denomina "*National Information Market*". En este modelo de mercado los titulares de datos retendrán la propiedad sobre su información personal y tendrán el derecho, pero no la obligación, de vender su información (ya sea en forma agregada o individual). Los pagos que se efectúen pueden darse a los individuos como una suerte de dividendo. Aquellos individuos que encuentren que los costos de perder su privacidad son mayores que los dividendos, se saldrán del mercado, aquellos que se sientan debidamente compensados, permanecerán en él. Este mercado que plantea Keneth Laundon es de cierta forma un modelo basado en una entidad certificadora: el "*National Information Market*".

Finalmente, podemos rescatar ciertos elementos comunes de los modelos de protección revisados, así:

- La asignación de las titularidades debe ceder a favor del titular de los datos personales. El sistema que ha de imperar por regla general es el *opt-in*. Es decir, se requiere el consentimiento previo del titular de los datos, para efectuar su tratamiento.
- El modelo debe distinguir entre los distintos tipos de datos personales que son tratados en el mercado, de manera que sea eficiente.
- Se deben establecer reglas de responsabilidad que desincentiven al que efectúa tratamiento de datos a infringir la normativa aplicable.
- El control del titular de los datos debe estar presente también en el mercado secundario de datos personales.

[19] PRIVACY RIGHT. Control of personal information. The economic benefits of adopting an enterprise-wide permissions management plataform. Privacy right white paper. 2001 [en línea] <http://www.privacyright.com/info/economic.html > [consulta: 10 febrero 2005]

[20] Keneth LAUDON, op.cit. pág. 1.

4.- PROPUESTA CONCRETA DE MODIFICACIÓN AL MODELO REGULATORIO CHILENO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Como se ha podido observar de lo indicado en la sección II del presente trabajo, nuestro marco regulatorio no es uno que asigne en forma clara y eficiente los derechos que en este ámbito se encuentran en disputa: el derecho a tratar datos personales vs el derecho a la privacidad informacional; existen bastantes hipótesis fácticas en las cuales no queda claro en qué persona radica el derecho, como asimismo, han quedado fuera de regulación, casos que necesariamente se han debido de tomar en cuenta, como lo ha hecho el derecho comparado[21]; asimismo, hay aspectos como el tratamiento de datos en el mercado secundario y la transferencia transfronteriza de datos que han quedado sin regular, y que claramente provocan que el mercado no sea eficiente[22], entre otros. Lo anterior, no propende a que exista en este mercado una asignación de recursos que maximice el valor de la actividad y el objeto regulado, de otra parte, produce costos de transacción elevados en el ámbito contractual, y genera sistemas de responsabilidad civil, en el extracontractual, que no cumplen con la finalidad pretendida por la norma. Además, existen ciertas fallas en el mercado de datos personales en Chile, las cuales pueden ser corregidas a través de la modificación de la normativa que regula la materia, en la forma que se propondrá en nuestro modelo de autonomía.

El estado actual de la situación muestra que si bien existen reglas legales que aplican al mercado de datos personales en nuestro país, los datos personales que se comercializan, lo son muy generalmente sin autorización por parte de los titulares de datos respectivos, de manera que éstos no pueden controlar su información personal (cómo, dónde y para qué se utilizará), y, además estos sujetos no son compensados por el uso de la información que les pertenece, ya que las empresas pueden recolectar libremente con la finalidad de utilizar o revelar información

[21] Así, por ejemplo, no existe en nuestra Ley 19.628 una excepción a la regla general de la autorización previa del titular que se refiera al tratamiento de datos que resulta necesario de la consecución de un negocio. Así lo hacen el Art. 6 N°2 de la LOPD española (1999. Ley Orgánica 15/99, de Protección de Datos de Carácter Personal de 1999), cuando indica que "No será necesario el consentimiento cuando los datos personales se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento y cumplimiento" y el Art. 5 letra d) de la Ley 25.326 de Protección de Datos Personales argentina, que indica que no se requerirá consentimiento cuando los datos "deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento".

[22] A este respecto basta mencionar que diversos inversionistas europeos que quisieron instalar *Call Center* en Chile para prestación de servicios en Europa, se han encontrado con el inconveniente que no pueden instalar este negocio en Chile, que supone tratamiento de datos personales, debido a la ausencia de un nivel de protección adecuado de cara a las exigencias de la Unión Europea. Algunos de ellos han solucionado este vacío a través de la suscripción de contratos- acuerdos previstos en la Directiva Europea que rige la materia, así como en la legislación interna de algunos de los países miembros, sin embargo, esta solución no satisface a algunos de los inversionistas que no están dispuestos a suscribir este tipo de contratos-acuerdos, de una parte debido al desconocimiento de las normas aplicables y, de otra parte, porque la infracción del contrato-acuerdo implica que las multas que se les pueden aplicar por el Organismo de Control europeo respectivo son altas. En cambio, si Chile cumpliera con la norma, en caso de incumplimiento, las multas a aplicar conforme estas normas serían las chilenas, las cuales son comparativamente mucho más bajas que las que contemplan las legislaciones europeas, por lo que los inversionistas prefieren que Chile homologue su legislación interna, y postergar, o simplemente no efectuar la inversión. Entrevista efectuada con fecha 30 de marzo de 2006 a Alberto Cerda Silva, Asesor Jurídico de la División Tecnologías de la Información de la Subsecretaría de Economía, Fomento y Reconstrucción.

personal en una o múltiples ocasiones sin tener que pagar ninguna compensación[23]. En definitiva, en nuestro ordenamiento no existe norma legal que entregue a los individuos un derecho de gozar 'exclusividad' sobre su propia información personal.

Frente a lo anteriormente expuesto, planteamos en base al Teorema de Coase, una asignación de titularidades protegidas por derechos de propiedad a los titulares de datos personales, lo que, desde ya prevenimos, no se efectúa en todas la hipótesis de tratamiento de datos, debido a que hay casos en que es eficiente que la asignación de los derechos de propiedad sea entregada a aquellos que desean tratar datos personales. En este escenario, la existencia de una entidad certificadora de datos personales puede ayudar mucho a que el mercado de datos personales sea eficiente. La entidad certificadora, es una entidad privada que sirve de aglutinadora de información personal, los titulares de datos que se encuentren interesados podrán concurrir a esta entidad y certificar sus datos, a través de un procedimiento en el cual la entidad se cerciora de la veracidad de los datos que son entregados por el titular, comprando a este último la referida información, y adquiriendo además, el sujeto titular de los datos, la obligación de mantener la referida información personal actualizada, con lo cual se asegura que los datos sean de calidad, y los titulares de ellos compensados. Luego aquellas empresas, entidades u organismos gubernamentales que estuvieren interesados en obtener datos personales de un determinado sujeto, recurrirán a la entidad certificadora a comprar esta información que es de calidad. Debemos acá hacer referencia a aquellos sujetos que nunca van a certificar sus datos: ¿qué pasa con esa información que ya no estará –a lo menos en este mercado certificado-? Lo que ocurrirá es que las empresas y el sistema en general establecerán una suerte de presunción en contra de este sujeto, sobre la base de que si no ha entregado voluntariamente sus datos personales y no se ha certificado, es porque, no es conveniente para él que su información se conozca, luego estas entidades no estarán interesadas ya en la información de este sujeto porque presumirán que la información que le concierne es negativa a sus intereses.

El hecho que le entreguemos al titular de los datos la posibilidad de elegir si revela o no su información personal vs por medio de la ley exigir que lo haga, en donde no existe elección, genera de por sí, una asignación eficiente en la economía. En el esquema de Coase lo que debería ocurrir es que individuos que valoran poco su privacidad informacional y mucho el rol de su información en posibles contrataciones o transacciones futuras (seguros, salud, créditos, etc.) van a estar dispuestos a vender su información personal, ya sea al ente certificador o bien directamente al interesado en sus datos. Al contrario, el titular de datos que valora mucho su privacidad no entregará sus datos, y puede incluso llegar a pagar o prohibir el uso de su información personal (como por ejemplo, ocurre con el pago que es necesario efectuar para no aparecer en la guía telefónica, o cuando adquirimos programas computacionales que impiden el rastreo de nuestras visitas a Internet). De esta manera, si toda la sociedad elige lo que maximiza su beneficio personal por medio de la facultad que posee de escoger si revela o no sus datos personales, se generarán elecciones que son eficientes globalmente y dejando a la sociedad mejor desde un punto de vista de eficiencia económica, en vez de imponer una solución legal que les obligue a revelar o mantener ocultos sus datos personales.

En el presente acápite, efectuaremos una propuesta de modificación al modelo de protección de datos personales en nuestro país, para lo cual tendremos presente las críticas y deficiencias observadas anteriormente. Este modelo lo llamaremos Modelo de Autonomía, pues se encuentra cimentado fundamentalmente en la voluntad del titular de los datos. Contiene elementos que resultan esenciales: i) Propietarización; ii) Contratos; iii) Asignación de derechos y reglas de pro-

[23] En este escenario la información personal tiene algunas de las características de un "bien público", y como tal, está extensamente disponible.

tección; iv) Control del titular de los datos personales; v) Responsabilidad y régimen sancionatorio, los que pasaremos a revisar a continuación.

4.1.- PROPIETARIZACIÓN

Como ya hemos examinado, varios autores han planteado un enfoque respecto a la privacidad que se encuentra estructurado en base al mercado, lo que llevaría a proteger la información personal. Como señala Ann CAVOUKIAN[24] la razón principal de ello es que la información personal es un bien, y por lo tanto, se debe intercambiar en un mercado bien estructurado. Esta visión se basa en un mercado exento de fallas, en el cual los individuos pueden escoger renunciar a algo de su privacidad si fueran compensados adecuadamente por su pérdida, lo cual se lograría a través del establecimiento de derechos de propiedad sobre la información personal.

Al asignar derechos de propiedad sobre la información personal a los individuos, se eliminaría la característica de "bien público" que ésta posee. En vez de eso, la información personal llegaría a ser un bien con valor comercial, y como tal, se compraría y sería vendida por un mecanismo de precios, permitiendo a los individuos encontrar un precio apropiado al cual desean vender, y permitiendo a las empresas encontrar un precio al cual desean comprar[25]. De lo anteriormente señalado por Ann CAVOUKIAN, cabe preguntarse si actualmente no estamos ya en este mundo, en el cual los datos personales tienen un valor comercial y son transados en el mercado. La respuesta es que sí, efectivamente constituyen un bien desde un punto de vista económico, y más específicamente uno cuasi-privado, desde que la exclusión es posible. Sin embargo, y no obstante transarse en el mercado los datos personales, una de las partes que debiera participar de la transacción sobre ellos, no lo está haciendo, esta parte es el titular de los datos, quien rara vez es compensado por el uso y/o venta de su información personal. Lo que hace pensar que en nuestro país no existe una asignación de derechos de propiedad al titular de los datos, pues de lo contrario, éste sería compensado, y podría ex-ante, proteger sus intereses.

Siguiendo con el análisis, si hipotéticamente asignamos inicialmente a los titulares de datos los derechos de propiedad sobre su información personal, aquellos que efectúan tratamiento de datos personales tendrían la posibilidad de transar con el individuo para obtener sus datos. Se produciría, entonces, una distribución de derechos entre los titulares de datos y aquellos que los adquieren, con la obtención de un derecho que se podría utilizar en el mercado. Bajo estas condiciones, el titular y el interesado en los datos personales negociarían por sus intereses, y este último tendría que pagar la compensación si quiere obtener información personal del titular de datos.

Si bien es cierto que el modelo de propietarización expuesto se encuentra íntimamente ligado al mercado como mecanismo de protección de la privacidad, no es menos cierto, que la asignación de derechos de propiedad en la información personal es necesario efectuarla a través de la norma. Es más, en realidad, ya existe una ley que acompaña al mercado en nuestro país, el tema es si la combinación es la mejor y, si no, cómo la ley debe estructurar el mercado. Como hemos observado de lo reseñado hasta acá, la combinación no es la mejor, de manera que resulta fácil concluir que ésta puede ser mejorada, a través de modificaciones a la normativa nacional aplicable a la materia, que recojan los elementos del modelo de autonomía que se plantea.

[24] Ann CAVOUKIAN, 1999. Privacy as fundamental human right vs. an economic right: an attempt of conciliation. [en línea] <http://www.ipc.on.ca/docs/pr-right.pdf> [consulta: 26 febrero 2006] pág. 18.

[25] Ibídem.

4.2. CONTRATOS

En el mercado de datos personales, intervienen a lo menos tres sujetos: el titular de los datos; el titular del banco de datos; y, el adquiriente final de la información. Nuestro modelo requiere que estos sujetos transen la información personal a través de contratos que regulen la compra, uso y posteriores usos de los datos personales, esto último implica que se regule el mercado secundario de datos personales.

Uno de los temas fundamentales a indicar acá es la distinción primaria que ha de efectuarse entre aquellos casos en que el titular de los datos y el eventual adquiriente de su información personal están alineados, esto es, el titular de los datos desea comunicar o ceder sus datos personales en determinadas condiciones, estando, a su vez, el tercero interesado en poseer esa información personal en las condiciones que indica el titular de los datos, y aquellos otros casos, en que un potencial adquirente de datos personales desea poseer cierta información de naturaleza personal, pero su titular no está dispuesto a comunicarlos, cederlos o transarlos voluntariamente. En el primer caso, las partes llegarán -dadas ciertas condiciones- a la celebración del contrato correspondiente; en el segundo, simplemente tal acuerdo no existirá.

En todo momento, los agentes económicos efectúan un análisis costo-beneficio sobre la maximización de su utilidad/beneficios. De esta manera, si el titular de los datos está dispuesto a pagar más para que sus datos se mantengan privados de lo que está dispuesto a pagar el potencial adquirente de esos datos por poseerlos, entonces el titular de los datos deberá pagar a este último por mantener los datos privados. En cambio, si el adquirente valúa más esos datos, o está dispuesto a pagar más por ellos, de lo que lo valúa el titular de los datos, entonces él pagará por que los datos ya no se mantengan privados. En ambas situaciones deberá existir un acuerdo o contrato de por medio.

Una vez asignados los derechos de propiedad, ya sea en el titular de los datos o bien en el que efectúa el tratamiento de ellos, los contratos aparecen como un buen medio para solucionar los problemas de privacidad informacional, ya que primeramente se pueden asignar los derechos de propiedad sobre la información personal a los titulares de ellos, pero luego, permitir que esa información sea usada por tiempo limitado y para determinados propósitos por otros[26].

Debemos tener presente en nuestro modelo los costos de transacción; el tema se nos presenta así, bajo la óptica de Coase: En un escenario en donde los costos de transacción son nulos, no es relevante la asignación inicial de derechos que haya efectuado la ley o si ésta no ha hecho ninguna, ya que las partes igualmente a través de los contratos llegarán a un resultado eficiente. En cambio, en un escenario en el cual los costos de transacción son elevados o importantes, sí importa que la asignación inicial de derechos sea eficiente, ya que las partes por sí solas, dados los costos de transacción, no lo logran. Consecuentemente, y dado que la regulación de datos personales actualmente no asigna eficientemente los derechos, la solución óptima es modificar la legislación, debido a que en el mercado de datos personales sí existen costos de transacción. Ahora bien, siempre los contratos serán una herramienta esencial para reasignar o redefinir los derechos de propiedad que no han sido asignados eficientemente en un principio, ya sea por una mala regulación legal o bien porque los sistemas autorregulatorios no funcionan. Es por lo anterior que en nuestro modelo de autonomía la existencia de contratos entre las partes resulta esencial, no sólo en la primera transacción entre las partes, sino sobre todo en el mercado secundario, ya que ellos permiten al titular de los datos mantener control respecto de su información personal, en los sucesivos usos de ella.

[26] Ver Hal VARIAN. 1996. *Privacy as fundamental human right vs. an economic right: an attempt of conciliation*. [en línea] <http://www.sims.berkeley.edu/~hal/Papers/privacy/> [consulta: 02 febrero 2005].

Concluyendo, para que las transacciones sobre los datos personales (contratos) puedan ocurrir eficientemente, hay varios requisitos previos: Costos de transacción suficientemente bajos[27]; una normativa que permita que los contratos se suscriban; simetría de la información entre las partes de la negociación; y la existencia de derechos de propiedad sobre la información personal.

4.3. ASIGNACIÓN DE DERECHOS Y REGLAS DE PROTECCIÓN

La asignación de derechos es sólo el principio de una interacción mucho más compleja. Algunas personas pueden querer y poder necesitar más privacidad informacional que otros, y por otra parte, algunas personas querrán acceder más que otras a información personal, por lo tanto, qué elementos debemos considerar al momento de asignar los derechos es una pregunta cuya respuesta resulta esencial. Coase indica que en un conflicto entre las preferencias de dos individuos cuando los costos de transacción son importantes, la asignación de derechos debe ser entregada a quien sea *"least cost avoider"*, es decir, la parte que puede resolver el conflicto al menor costo posible o a la parte que más valúa el derecho[28], dependiendo cuál de estas dos variables sea más fácil medir en un momento determinado. Creemos que en ambos casos, es al titular de los datos a quien se le deben asignar los derechos de propiedad, en primer lugar debido a que ellos incurren en un menor costo ante el conflicto, ya que basta para ellos decidir si se ceden o no sus datos personales vs. el costo en que incurren los que desean acceder a los datos personales, debido a que existen mayores trabas para que puedan acceder a la información de los individuos (efectuar procesos de recogida de datos, cerciorarse de la veracidad de los datos, establecer la pertinencia de los datos que recolectan, etc.), incluso existirán ocasiones en que deberán tener que pagar para obtener esa información personal, todo lo anterior, si y sólo si el titular de los datos personales no está dispuesto a ceder su información personal y, en segundo lugar, porque la privacidad informacional es mucho más valorada por los propios propietarios de ésta vs. el valor que le pueda asignar a la privacidad de otro una empresa o entidad. En la práctica la asignación del derecho a la privacidad informacional, protegido por reglas de propiedad, implica la imposibilidad de efectuar tratamiento de datos, sin el previo consentimiento del titular de ellos.

Sin embargo, debemos tener presente que existen excepciones a lo anteriormente expuesto, en razón de las cuales entregaremos al titular del banco de datos la titularidad, como se podrá observar de lo señalado en el modelo de autonomía propuesto.

Una vez realizada la asignación inicial de derechos por la ley, debemos, conforme lo señalan Calabresi y Melamed, determinar la regla de protección adecuada entre reglas de propiedad, responsabilidad e inalienabilidad.

Compartimos lo señalado por Lawrence Lessig[29], quien afirma que en el ámbito del tratamiento de datos personales, un régimen de reglas de propiedad es mucho más adecuado que uno basado en reglas de responsabilidad. Si se asignan derechos de propiedad a las personas, éstas podrían disponer tanto de la capacidad de negociar con facilidad sobre sus derechos de privacidad informacional, como inicialmente de la titularidad de la privacidad. Los individuos

[27] Respecto de este requisito cabe señalar que las tecnologías no solamente constituyen un elemento que facilita el tratamiento de datos personales, sino que también, uno que aminora los costos de transacción al poder las partes negociar con mayor facilidad, rapidez, y en mayor cantidad.

[28] Al asignar los derechos de propiedad a la parte que los valúa más, la ley vuelve innecesario el intercambio de derechos y así ahorra el costo de una transacción. Robert Cooter y Thomas Ulen, 1999. Derecho y economía. 1ª reimpresión. México D.F., Fondo de Cultura Económica. 686 p., pág. 129.

[29] Lawrence Lessig, 2001. El código y otras leyes del ciberespacio. Madrid, Taurus. 544 p., pág. 295.

debieran disponer de la capacidad de controlar la información sobre sí mismos. Este autor señala las siguientes diferencias, entre un régimen y otro:

a) En el régimen de propiedad es necesaria una negociación antes de obtener algo, mientras que el régimen de responsabilidad permite obtener primero y pagar después (a título de indemnización).

b) La clave en un régimen de propiedad es proporcionar el control y el poder a la persona que ostenta el derecho de propiedad, mientras que la clave en un régimen de responsabilidad es proteger el derecho pero facilitar la transferencia de un bien entre una persona y otra. Así la propiedad protege la posibilidad de elegir, la responsabilidad protege la transferencia.

c) Mediante reglas de responsabilidad, un tribunal o la ley determina el valor que los datos personales y la privacidad tienen para el individuo. En cambio, cuando alguien posee un derecho de propiedad, resguardado por reglas de propiedad, toda aquella persona que desee algo de su propiedad deberá negociar el precio antes de poder obtenerlo. Por consiguiente, un régimen de propiedad protege tanto a aquellos que valoran su privacidad por encima de los demás como a los que la valoran por debajo de los demás, obligando a quienes deseen obtener un recurso dado a preguntar antes de tomarlo. Un régimen de este tipo otorga la confianza en que, si va a haber una negociación de por medio, el trato se sellará a un precio que resulte óptimo para las dos partes.

De nuestra parte, creemos que las reglas de propiedad resultan adecuadas como forma de protección de la asignación de derechos a los titulares de datos, ya que tenemos la certeza que éstos son *"least cost avoiders"* y que valoran más su privacidad informacional que los que desean tratar sus datos.

Relacionado con la regla de protección escogida nos encontramos con el régimen de compensaciones. Las compensaciones por el uso del tratamiento de datos se pueden dar en dos instancias; una compensación que denominaremos *ex–ante* en razón de la cual el titular de los datos y el responsable del banco de datos transan la información que le concierne al titular de los datos, produciéndose una entrega de información de una parte (a lo menos una entrega, pueden existir otras obligaciones, como por ejemplo, una obligación de actualización de los datos personales entregados), y de otra un pago (compensación) por la prestación recibida; la segunda instancia de compensación, que denominamos *ex-post*, que se puede producir ante un tratamiento de datos, es aquella que nace del tratamiento indebido o ilegal de ellos, que da origen a compensaciones que tienen una naturaleza indemnizatoria por los daños o perjuicios causados del referido tratamiento ilegal o indebido.

Las compensaciones *ex–ante* se darán siempre en los casos de protección vía reglas de propiedad, en la medida en que exista acuerdo entre las partes, haciendo que el titular de la información personal actúe en el mercado, siendo debidamente compensado. En cambio, en un régimen de protección basado en reglas de responsabilidad, la compensación es eventual y *ex - post*, ya que sólo operará cuando el tratamiento de datos cause un perjuicio al titular de ellos, debiendo asumir una serie de costos asociados, como por ejemplo los judiciales, para el caso de pretender cobrar los daños causados.

Finalmente, una de las reglas de protección señaladas por Calabresi y Melamed de la asignación de titularidades es la inalienabilidad, la cual entenderemos a los efectos de los datos personales como cualquier restricción en la transferencia, propiedad o uso de la información personal, como cualquier restricción contraria a los deseos del titular de los datos. De esta manera, si la sociedad escoge una regla de inalienabilidad ya sea total o parcial, los titulares de datos verán limitado su

derecho a enajenar su información personal; por el contrario, si la regla es la libre alienabilidad, los titulares de los datos personales podrán enajenarlos en la forma que deseen[30].

Por último, cabe señalar que existen derechos que son protegidos por reglas de protección mixtas, esto es, un mismo derecho puede ser o potencialmente ser protegido por dos o más reglas.

Podemos resumir las asignaciones de derechos y las respectivas reglas de protección en materia de protección de datos[31] en el esquema siguiente:

Derecho a la privacidad informacional protegido por reglas de propiedad.

"X" no puede tratar datos personales, salvo que el titular de los datos lo permita. El titular de los datos puede prohibir el perjuicio causado por "X".

Derecho a la privacidad informacional protegido por reglas de responsabilidad.

"X" puede tratar datos personales, pero debe compensar al titular de los datos por los daños efectivamente causados.

Derecho a tratar datos personales protegido por reglas de propiedad.

"X" puede tratar datos personales a voluntad, sólo puede ser detenido por el titular de los datos si éste le paga, esto es, si le compra el derecho. (el tratamiento de datos no es considerado perjuicio para el titular de los datos).

Derecho a tratar datos personales protegido por reglas de responsabilidad.

"X" puede tratar datos personales, pero el titular de los datos puede obligar a "X" a dejar de tratar datos, pero si lo hace debe compensar a "X".

4.4.- LA ASIGNACIÓN DE DERECHOS EN LA NORMATIVA CHILENA VIGENTE

Para el caso concreto de la legislación chilena en materia de tratamiento de datos, debemos distinguir a efectos de verificar bajo qué reglas de protección se encuentran amparados los derechos, si el tratamiento en cuestión ha resultado indebido o ilegítimo, de manera que genera perjuicios al titular de los datos, o si el tratamiento de ellos, es legítimo. Asimismo, se establece una clasificación de las asignaciones de titularidades que efectúa la ley, en base a las distintas categorías de datos personales establecidos en la norma, la cual se efectúa tomando en cuenta el grado de control que tiene el titular de los datos (autorización).

I Asignaciones de derechos y reglas de protección en caso de tratamiento legítimo de datos.

a) Datos provenientes de fuentes accesibles al público.

   i. Datos patrimoniales.

   ii. Datos listados de personas.

   iii. Datos marketing.

   Derecho a la privacidad informacional protegido por reglas de responsabilidad.

b) Datos de personas jurídicas privadas.

[30] Ver SCHWARTZ, op. cit. pág. 2074.

[31] Teniendo presente que, como señalan Melamed y Calabresi, la mayoría de los derechos son mixtos.

Derecho a la privacidad informacional protegido por reglas de responsabilidad.

c) Datos patrimoniales negativos comunicables.

Derecho a la privacidad informacional protegido por reglas de responsabilidad.

d) Datos sensibles.

Derecho a la privacidad informacional protegido por reglas de propiedad.

e) Datos de salud sensibles.

Derecho a la privacidad informacional protegido por reglas de propiedad.

f) Datos médicos

Derecho a la privacidad informacional protegido por reglas de propiedad.

g) Datos penales.

Derecho a la privacidad informacional protegido por reglas de responsabilidad.

h) Datos públicos.

Derecho a la privacidad informacional protegido por reglas de responsabilidad.

i) Datos en general

   Derecho a la privacidad informacional protegido por reglas de propiedad.

II Asignaciones de derechos y reglas de protección en caso de tratamiento ilegítimo de datos.

En este caso, pasamos respecto a todos los tipos de datos a una regla de responsabilidad como vía de protección de la privacidad informacional.

4.5. ASIGNACIÓN DE DERECHOS Y REGLAS DE PROTECCIÓN BAJO EL MODELO DE AUTONOMÍA

En el entendido que la asignación de derechos y las formas de protección dependerán de diversas circunstancias en materia de privacidad informacional, como por ejemplo, el dato personal de que se trate y la finalidad del tratamiento es que plantearemos a continuación, un modelo de autonomía para el caso chileno que tome en cuenta no sólo lo planteado anteriormente respecto a los fundamentos para entregar la asignación de derechos al titular de los datos, sino también las excepciones que deben existir en este modelo. Creemos que plantear soluciones absolutas como un régimen de *opt-in*, autorización del titular, prohibición de tratar datos personales o como quiera llamársele, sin el establecimiento de excepciones adecuadas, no constituirá en ningún caso, un modelo eficiente, ya que puede dejar a la economía sin la información necesaria para tomar decisiones informadas o al gobierno sin las herramientas que le permitan realizar políticas públicas.

4.5.1. Asignaciones y reglas de protección en caso de tratamiento legítimo de datos en el modelo de autonomía.

a) Datos patrimoniales positivos: Entendemos como tales todo dato de carácter económico, financiero, comercial o bancario que se refiera al patrimonio de una persona, que dé cuenta de sus activos, como por ejemplo: propiedades, bienes, etc.

En este caso, se otorgará al titular de los datos un derecho a la privacidad informacional protegido por reglas de propiedad. Lo anterior debido a que en este caso no es necesario generar un incentivo para que los titulares de los datos entreguen sus datos patrimoniales, debiendo en consecuencia, mantenerse la regla general expuesta en nuestro modelo.

b) Datos de marketing o con fines publicitarios: Estos datos son aquellos que se tratan con el objeto de efectuar prospección comercial, venta directa de bienes y/o servicios o comunicaciones comerciales de respuesta directa.

Respecto de este tipo de datos se asigna al titular de los datos personales el derecho a la privacidad informacional protegido por una regla de propiedad. Lo anterior, ya que otorgar el derecho a los titulares de los bancos de datos, implicará una sobreproducción de información, por otra parte, si asignamos el derecho al titular de los datos, el marketing que se efectúe será mucho más eficiente, desde que se efectuará un marketing dirigido, en el cual los titulares de datos sólo recibirán aquella información que les interesa, haciendo que esta actividad sea mucho más eficiente.

c) Datos sensibles: Entenderemos por tales aquellos datos personales cuyo conocimiento por parte de un tercero, pueden implicar la toma de decisiones discriminatorias y arbitrarias respecto del titular de los datos. Entendemos comprendidos dentro de este tipo de datos, aquellos relativos a la vida sexual, afiliación política o sindical, raza, creencias religiosas, estados de salud físicos y psicológicos, historial penal o criminal.

Al titular de los datos sensibles se le asignará el derecho a la privacidad informacional, protegido por reglas de propiedad. La anterior asignación debe efectuarse al titular de los datos, ya que de no realizarse de esta manera, pueden tomarse decisiones que resulten arbitrarias y discriminatorias, que no miren a criterios de eficiencia.

d) Datos en general: Dentro de esta categoría de naturaleza residual, encontramos todos aquellos datos que no se encuentran comprendidos dentro de las categorías anteriores.

Aplicamos acá la regla general de nuestro modelo: derecho a la privacidad informacional protegido por reglas de propiedad.

4.5.2. Excepciones a las asignaciones y reglas de protección indicadas

Como ya lo hemos indicado anteriormente, en el modelo de autonomía, existen excepciones a las reglas anteriormente expuestas, las que revisaremos a continuación:

a) Datos patrimoniales negativos: Son datos de este tipo todos aquellos que sean de carácter económico, financiero, comercial o bancario y que den cuenta de los pasivos del patrimonio de una persona.

En esta hipótesis, se otorgará el derecho a tratar datos al titular del banco de datos protegido por una regla de inalienabilidad parcial. Nos alejamos acá de la regla general, debido a que no existirá por parte de los titulares de datos patrimoniales negativos el incentivo a entregar información que le es adversa. La regla de la inalienabilidad parcial implica que los titulares de bancos de datos, aun cuando tengan el derecho de tratar datos, no pueden vender a los titulares de datos respectivos este derecho, ya que permitir hacerlo, implicaría un contrasentido en el modelo, debido a que los titulares de estos tipos de datos comprarían sus datos patrimoniales negativos con el objeto de no aparecer en las bases de datos de sujetos incumplidores. Y es parcial la inalienabilidad, porque los titulares de estos bancos de datos tendrán que eliminar o cambiar los referidos datos, cuando la información negativa de la que dan cuenta cambie.

Este modelo de autonomía ha sido estructurado pensando en su posible implementación al corto plazo, debido a que cuando no se aplica la regla general, los derechos son entregados al titular del banco de datos, lo cual llevaría a la sociedad a un equilibrio eficiente. Sin embargo, existe un *primer mejor* para la sociedad caracterizado por la introducción de una entidad certificadora, que ya fuera descrita, y que logrará volver a la regla general en el caso de los datos patrimoniales negativos, donde a pesar que el derecho a la privacidad informacional sea entregado ahora a los titulares de los datos, existirá por parte de éstos el incentivo a estar certificados, debido a que la lectura que hace el mercado de los individuos no certificados es adversa, de manera que cuando exista certificación será muy extraño que existan personas que se marginen de este sistema, con lo cual finalmente será casi universal estar certificado. Logrando finalmente un equilibrio eficiente para la sociedad, sin imposición.

b) Fuentes accesibles al público: En el modelo de autonomía serán fuentes accesibles al público aquellas que hayan sido establecidas como de carácter no reservado por una norma legal o reglamentaria. De esta manera, y en el ordenamiento actual vigente, podrían tratarse los datos patrimoniales positivos, sin la autorización previa del titular de los datos, que se encuentren en este tipo de fuentes, como por ejemplo, los registros de propiedad del Conservador de Bienes Raíces.

c) Contratos y relaciones negociales: Asimismo, no será necesario el consentimiento del titular de los datos en aquellos casos en que el tratamiento de ellos sea necesario para mantener o cumplir un contrato o una relación negocial, laboral o administrativa.

d) Tratamiento ilegítimo o indebido de datos: En este caso nuestra regla general sufre un cambio, ya que si bien el derecho de privacidad informacional es asignado al titular de los datos, la regla de protección varía de una de propiedad a una de responsabilidad, ya que en este caso la compensación por el uso (o, más bien, mal uso) de los datos personales se producirá *ex–post*, habiendo existido o no un contrato previo entre las partes involucradas.

e) Tratamiento por órganos públicos: Se entregará a los órganos públicos, sin autorización del titular de datos respectivo, el derecho a tratar datos personales protegido por reglas de inalienabilidad, cada vez que el tratamiento de la referida información personal sea necesaria para cautelar los intereses del individuo en el ejercicio de las funciones propias de los órganos públicos respectivos.

4.6. CONTROL DEL TITULAR DE LOS DATOS PERSONALES

Nuestro modelo de autonomía entrega el control de la información personal a los titulares de los datos personales, este control se hace efectivo en la práctica a través de dos mecanismos, a saber: la autorización o consentimiento y los derechos subjetivos del titular de los datos.

4.6.1 Autorización o consentimiento.

A nuestros efectos entenderemos a la autorización o consentimiento, como la libertad de escoger entre alternativas u opciones, en una base informada, y en ausencia de coerción. Implícito en el hecho de autorizar el tratamiento de datos personales está el requisito que el individuo

tenga el conocimiento o la información suficiente para ser capaz de hacer una elección informada. La información personal es vista por los individuos como algo que les pertenece y, por lo tanto, ellos sienten que tienen el derecho de decidir si la revelarán, y a quién[32].

La información puede ser utilizada y revelada interminablemente. En estas condiciones, la posibilidad de un individuo para ejercitar el control y tener el real control con respecto a cómo su información personal se puede utilizar es limitada. Desde la perspectiva del individuo su habilidad para ejercitar el control sobre su información se ve restringida debido a que, como dirían los economistas, existe "asimetría de información y de poder de negociación". Por lo tanto, los individuos necesitarían poseer bastante información acerca del mercado y del valor de su información personal para determinar cómo su información se manejará y cuál es el valor comercial que puede tener. Adquirir este conocimiento para todas las transacciones que un individuo hace en el curso del tiempo requeriría una gran inversión de tiempo y energía. En otras palabras, al tratar con información asimétrica, los individuos necesitan tener disponible suficiente información sobre las prácticas institucionales para ser capaz de tomar una elección informada en cuanto a si efectuar o no transacciones con una institución que efectúa tratamiento de datos personales. Bajo estas condiciones existentes en el mercado, los individuos están actualmente en una situación desventajosa para ser capaces de controlar o negociar las fronteras de su privacidad[33]. Una solución es entregar a través de la norma la posibilidad al sujeto de tomar decisiones informadas. Lo anterior requiere de los siguientes cambios normativos:

- La existencia de un registro de bancos de datos privados, que permita al titular de los datos saber quién, cómo y de qué manera está tratando sus datos personales, como asimismo, le permitirá transar con aquellos titulares de bancos de datos que aparezcan en el referido registro. Cabe recordar que nuestra legislación sólo establece la existencia de un registro de datos públicos.
- La autorización o consentimiento del titular de los datos, no sólo debe ser un consentimiento inicial, sino que además, debe consentir en las eventuales futuras cesiones de los datos personales respecto de los cuales ha autorizado inicialmente su tratamiento. Nos referimos acá al mercado secundario de datos personales; en este mercado, también el titular de los datos debe tener control. La legislación vigente en Chile, respecto a este punto guarda silencio, de manera que los futuros usos o cesiones de la información personal inicialmente obtenida o tratada no requieren de la autorización del titular de los datos.
- El sujeto debiera tener siempre la posibilidad de revocar su autorización o consentimiento, salvo que contractualmente se haya obligado a no revocar por un tiempo determinado. Sin embargo, este tiempo no debiera ser lo suficientemente largo para permitir que las condiciones en que se prestó el referido consentimiento cambien de manera importante, ya que de ser así, la revocación ha de ser posible.
- Las eventuales futuras cesiones o transferencias de los datos respecto de los cuales fue originalmente consentido su tratamiento, no debieran variar respecto a la finalidad del tratamiento inicialmente consentida. De lo contrario, el titular de los datos, debiera tener el derecho de revocar su autorización y/o de no consentir en la referida cesión.
- El titular de los datos, finalmente, debe ser informado no sólo de la finalidad del almacenamiento de sus datos personales y su posible comunicación al público, sino que también,

[32] Ver. PRIVACY RIGHT. *Control of personal information. The economic benefits of adopting an enterprise-wide permissions management plataform. Privacy right white paper.* 2001 [en línea] <http://www.privacyright.com/info/economic.html > [consulta: 10 febrero 2005].

[33] Ibídem.

de otros aspectos que resultan relevantes a la hora de determinar por parte del titular de los datos la venta o autorización de sus datos personales; así, se le debiera informar respecto de la entidad que tratará su información personal, qué tipo de tratamiento se efectuará respecto de ella, y el tiempo por el cual se hará.

- Respecto a aquellos documentos o fuentes de información personal respecto de la cual no existe sólo un titular, ya que por ejemplo, han sido creadas o contienen datos de más de una persona, por ejemplo, en el caso de un contrato o de una receta médica, será necesario el consentimiento de todos los titulares de datos involucrados.
- Por último, creemos en la posibilidad de que existan consentimientos o autorizaciones generales para efectuar tratamiento de datos personales, siempre que se cumplan con todos los requisitos expuestos anteriormente.

4.6.2. Los derechos subjetivos.

El principio de calidad de los datos personales, esto es, que los datos que sean tratados sean exactos de manera que reflejen el verdadero estado actual del que dan cuenta, exige que la norma legal le entregue a los titulares de datos personales una serie de derechos subjetivos no solamente en miras de proteger su información personal sino que también en aras de un funcionamiento eficiente del mercado de datos personales.

Por otra parte, se debe establecer la obligación para los titulares de bancos de datos personales de mantener datos de calidad. Lo anterior, en nuestro modelo de autonomía se puede obtener no sólo por medio de una obligación legal sino que también a través del establecimiento en los contratos que subscriban las partes de la obligación recíproca de mantención de datos de calidad. Así por ejemplo, el titular de los datos al vender su información personal puede obligarse con el titular del banco de datos respectivo a mantener permanentemente actualizada la información que ha sido vendida.

De otra parte, la ley en tanto norma supletoria debiera reconocerle a los titulares de los datos el derecho de exigir al banco de datos la eliminación o modificación de los datos cuando éstos ya no sean de calidad. Obligación de eliminación o modificación que, en todo caso y aun cuando el titular de datos no lo exija, debe pesar sobre los titulares de bancos de datos.

Finalmente, cabe mencionar que en esta parte nuestra legislación vigente en la materia cumple con lo aquí reseñado.

4.7. RESPONSABILIDAD Y RÉGIMEN SANCIONATORIO

En nuestro modelo de autonomía, el tema de la responsabilidad por el tratamiento indebido o ilegítimo de datos, debiera resolverse con cláusulas de responsabilidad por incumplimiento contractual y con normas supletorias legales.

Respecto de las normas supletorias legales creemos que no existen motivos para cambiar el actual régimen de responsabilidad por culpa establecido en la Ley 19.628, y que por lo demás, es el general en nuestro ordenamiento.

Sí creemos que las multas que establece la citada ley para la falta de entrega oportuna de información o el retardo en efectuar la modificación en la forma decretada por el tribunal, que son de 2 UTM a 50 UTM, son del todo ineficaces ya que no incentivan a los titulares de los bancos de datos a cumplir con la norma y con las obligaciones adquiridas con los titulares de datos personales en los contratos que se suscriban, de manera tal que tales multas debieran ser aumentadas a los mismos niveles existentes en el ámbito europeo, que van desde los 601 Euros

a 601.000 Euros. Asimismo, las referidas multas no sólo debiesen ser aplicadas para los casos expresamente contemplados actualmente en nuestra normativa, sino que para cualquier caso de infracción a la norma o al contrato.

4.8. OTROS ASPECTOS A CONSIDERAR EN EL MODELO DE AUTONOMÍA

De las críticas expuestas a la legislación nacional, aun queda por pronunciarnos respecto de las siguientes:

- Debe existir un reconocimiento que valide a los códigos deontológicos o de conducta como instrumentos que suscritos o consentidos por las partes tengan un carácter vinculante para ambas.
- Respecto a la inexistencia de normas que regulen la transferencia transfronteriza de datos, es claro que nuestra legislación debe adoptar en esta materia lo establecido en el ámbito del derecho comparado, estableciendo niveles de protección adecuados, que incentiven las inversiones extranjeras, cuya ejecución implique un tratamiento de datos personales.
- En relación a la existencia de un órgano de control, creemos que en base al modelo de autonomía planteado, la creación de tal órgano no será necesaria, ya que sólo implicará para el sistema mayores costos, lo que no logrará la eficiencia que se busca en este mercado.
- Finalmente, no encontramos razones para excluir de la protección que brinda la Ley 19.628 y de nuestro modelo de autonomía a las personas jurídicas, las cuales forman parte del mercado de datos personales, no sólo en tanto titulares de banco de datos, sino que también en tanto titulares de información que les concierne.

5.- CRÍTICAS

No obstante creer que, conforme lo señalado anteriormente, es viable y eficiente crear un modelo de mercado de datos personales en nuestro país distinto del actual y que se conforme a los parámetros señalados en este trabajo, se hace necesario mencionar ciertas críticas al modelo de propietarización, aplicables al modelo de autonomía planteado acá. Así, por ejemplo, la Electronic Privacy Information Center, institución que forma parte de los grupos promotores de la privacidad, ha señalado que "las negociaciones en el mercado de datos, producen invariablemente una desventaja para aquellos que no puede comprar suficiente privacidad y producirá una gradual disminución en el nivel de protección disponible al público en general".[34]

De su parte, Eli Noam[35] reconoce ciertas críticas a la propietarización de los datos personales y a la privacidad como parte del mercado. Las sistematiza en tres.

- La intimidad es un derecho humano básico y no sujeto a intercambio transaccional: Un derecho es meramente una asignación inicial. Se puede adquirir sin una carga y es distribuido universalmente a pesar de la riqueza, pero está en la naturaleza del ser humano poseer preferencias y necesidades que varían, y cambiar lo que ellos tienen por lo que ellos quieren.

[34] ELECTRONIC PRIVACY INFORMATION CENTER. *Pretty poor Privacy: An assessment of P3p and Internet privacy*. 2000 [en línea] < http://www.epic.org/reports/prettypoorprivacy.html> [consulta: 07 marzo 2005].

[35] Eli Noam, op.cit. pág. 12.

Así, lo queramos o no, las personas comercian continuamente sus derechos, ejerciendo un derecho fundamental, el derecho de la libre elección.

- Los consumidores no pueden valorar correctamente el valor de mercado de renunciar a su información personal: Una segunda objeción es que los consumidores poseen asimetrías de conocimiento relativo al valor de su información personal, y que ellos serían explotados continuamente. Sin embargo, tales asimetrías de información se extenderían también a todas las otras dimensiones de transacciones.
- El sistema de transacciones en la privacidad perjudica a los más pobres: Aquí, se cree que son especialmente los pobres, que sufren de presiones financieras e ignorancia, quienes venderán sus derechos de privacidad a individuos e instituciones más adineradas. Es verdad que las prioridades de las personas pobres a menudo no incluyen la protección de la privacidad. Por otro lado, la misma condición de pobreza puede ser poco atractiva para una intrusión comercial.

Lo anterior lleva a este autor a concluir acerca de la privacidad, en base principalmente a que la privacidad posee una variedad de implicancias, que no existe una regla o política única a seguir. En un escenario donde las transacciones no son fructíferas indica que existen fallas de mercado, quizás debido a la existencia de monopolio o altos costos de transacción, o donde las externalidades negativas son muy altas, las regulaciones pueden ser apropiadas. Al contrario, cuando las transacciones se efectúan no hay razón para la intervención del Estado, y por lo tanto, debe existir un esfuerzo por eliminar limitaciones contra tales transacciones.

Michael Froomkin critica la idea de propietarizar la información personal, ya que desde su punto de vista, tal propietarización no cambiará el estado actual de las cosas, fundamentalmente debido a los costos de transacción; señala este autor: "Las características estructurales del mercado hacen costoso para los individuos negociar cláusulas de privacidad, en cambio, el mercado actualmente hace poco costoso para el autor de las cláusulas tipo incluir la transferencia de los datos personales y el consentimiento para su uso"[36].

Por otra parte, Daniel Solove[37] indica que la solución de mercado para la privacidad se fundamenta en la propietarización de la información personal y en los contratos. Sus críticas pueden ser esquematizadas en los siguientes puntos:

- Si bien reconoce que los contratos pueden proteger la privacidad en las relaciones existentes entre partes, éstos no lo hacen respecto a invasiones a la privacidad efectuadas por terceros fuera de la relación contractual.
- Reconoce la existencia de problemas en el poder de negociación que presentan los titulares de datos personales ante sus empleadores, compañías; junto con considerar que la mayoría de las personas acceden a cláusulas estándar.
- Muy relacionado con el punto anterior, en aquellos casos en que se presenta la posibilidad de opción para el titular de los datos ésta es una opción "*take-it-or-leave-it basis*".
- Finalmente, el más fuerte fundamento para nosotros es la dificultad en determinar el valor de la información personal, de esta manera indica: "En un mercado que funciona bien, asumiendo la inexistencia de fallas en él, el mercado trabaja correctamente asignando el valor a la información personal. Pero el mercado de la privacidad no es uno que funcione bien,

[36] Michael Froomkin, 2000. *The Death of privacy?* Stanford Law Review. 52: 1461-1543. pág. 1535.

[37] Daniel Solove, 2004. The digital person. Technology and privacy in the information age. New York, New York University Press. 283 p., pág. 81.

y entonces la determinación del valor de la información es incierta"[38]. A lo anterior, habría que agregar dos características del mercado de datos personales que hacen que valorar los datos sea más complicado; la primera de ella es lo que los norteamericanos denominan como "*aggregation effect*", que se refiere a que el valor de un dato considerado individualmente es muy distinto al valor de ese dato cruzado con otros que permiten determinar el perfil de una persona; y el segundo, dice relación con lo que hemos llamado en este trabajo como mercado secundario de datos; para este autor, es difícil que el individuo sepa con certeza los futuros segundos usos de su información lo que hace que no pueda determinar correctamente su valor al transar sus datos en la primera transacción.

6.- CONCLUSIONES

Como habrá podido concluir el lector, el problema de la privacidad informacional está lejos de ser un asunto teórico o académico, es más, toca diariamente a todos y cada uno de aquellos que conformamos la sociedad chilena, ya sea en calidad de titulares de datos personales, o bien, como titulares de bancos de datos. El gran desarrollo del mercado de datos personales en nuestro país es una realidad, más aún teniendo presente la masificación de la utilización de las tecnologías de la información y comunicación.

Una de las principales problemáticas que existen a la hora de regular el tratamiento de datos personales, es la variedad de industrias que efectúan tal tratamiento, como también, los distintos tipos de datos personales que se encuentran disponibles en el mercado, como por ejemplo: los registros de salud; el historial crediticio; llamadas de teléfono de larga distancia; los registros de un proveedor de servicios Internet; las compras hechas por el correo o el teléfono directos; registros criminales, entre muchos otros. Por lo tanto, al momento de regular no podemos pensar en absolutos, se deben combinar tanto mecanismos de mercado como el actuar del Estado, a través de la ley, a objeto de obtener la eficiencia. En este mismo sentido, se debe recoger lo anteriormente expuesto sobre la diversidad de industrias y diversidad de datos personales existentes en el mercado a la hora de regular normativamente en estas materias.

De esta manera, es necesario efectuar un enfoque de solución diferenciado, en donde se reconozca que no existe una única solución para la protección de los datos personales, ya que las transacciones de mercado pueden engendrar protección a la información personal, pero hay también casos en donde los mercados pueden fallar o las transacciones no suceder. Por lo tanto, en ocasiones, el mercado proporcionará una solución, mientras en otros casos, se presentará la necesidad de una legislación o una interpretación más fuerte de la ley o su modificación. Así, por ejemplo, en aquellos casos en que las negociaciones entre las partes sean costosas o incluso imposibles, la regulación por el Estado a través de la ley puede ser más efectiva que los acuerdos contractuales.

Sumado a lo anterior, el asunto más importante en el debate es la resolución de la disyuntiva sobre quién debe poseer la titularidad sobre la información personal, esto es, en términos simples quién debe controlar dicha información. Por otra parte, se debe tener presente el uso de información personal para propósitos distintos a los que se reunieron, como un tema clave en la discusión acerca del mercado secundario en la información personal.

Se ha planteado acá un nuevo estado regulatorio basado en el Modelo de Autonomía expuesto. Este modelo establece como regla general la asignación de titularidades en el mercado de datos personales, al titular de los datos, protegido por reglas de propiedad, desde que éste es el "*least cost avoider*" y quien valora más su propia privacidad informacional. Asimismo, el modelo establece que es necesario propietarizar la información personal, como el mejor mecanismo para hacer más eficiente el mercado, desde un punto de vista económico. De otra parte, juega un rol preponderante la existencia de contratos entre las partes, en un marco en que el control que se le entrega al titular de los datos, es materializado a través de la autorización informada y la existencia de derechos subjetivos que le aseguran al titular de los datos el hacer efectivo el señalado control. El modelo considera un régimen de responsabilidad y sancionatorio que realmente incentiva el cumplimiento de las normas legales y de los contratos suscritos entre las partes involucradas en el tratamiento de los datos personales. Finalmente, se establecen excepciones a la regla general planteada basadas en la diversidad de las industrias y en los distintos tipos de datos personales existentes.

Creemos que el modelo planteado –que impone una modificación legal- es factible en el corto plazo desde que el costo de hacer transacciones en el mercado de datos personales bajo un escenario de fallas de mercado como la información asimétrica que generan problemas de selección adversa y de riesgo moral, es mucho menor que el costo administrativo de implementar el modelo de autonomía que se plantea. Sin embargo, existe el desafío a largo plazo de establecer un modelo que además incorpore una entidad certificadora, que producirá mayor eficiencia aun al mercado de datos personales, ya que los titulares de la información personal, bajo este régimen, se verán incentivados, sin imposición alguna, a entregar de manera fidedigna tal información.

La protección de la privacidad informacional a través de la propiedad, puede ser una postura que resulte muy debatible por muchos, y de hecho lo es, sin embargo, creemos que este modelo brinda mayor protección a la privacidad de los titulares de datos, en un mundo en que actualmente ya se recogen, utilizan y venden datos personales. Lo que busca el modelo de autonomía planteado es regular a través de la propiedad este mercado, de manera que éste sea eficiente desde un punto de vista económico y lo sea, también, desde la óptica de la privacidad informacional.

[38] Daniel Solove, op. cit. 87.