UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
ESCUELA DE GRADUADOS

LA REGULACIÓN DEL MERCADO DE DATOS PERSONALES EN CHILE

Tesis para optar al grado de Magíster en Derecho

PAULA JERVIS ORTIZ

Director: Felipe Irarrázabal Ph.

Santiago, Chile
2006

A José Tomás, mi familia, en especial a mi madre y a mi hermana por su apoyo incondicional.

TABLA DE CONTENIDOS

CAPITULO SEGUNDO

ANALISIS DE LA NORMATIVA NACIONAL EN MATERIA DE PROTECCION DE DATOS PERSONALES, EN ESPECIAL DE LA LEY 19.628

CAPITULO TERCERO

CARACTERIZACIÓN DEL MERCADO DE DATOS PERSONALES EN CHILE

CAPITULO CUARTO:

ANÁLISIS ECONÓMICO DEL MERCADO DE DATOS PERSONALES Y SU REGULACIÓN

ANEXO

GENERALIDADES DEL ANÁLISIS ECONÓMICO DEL DERECHO Y DE LA TEORÍA ECONÓMICA DE LA PROPIEDAD

INTRODUCCIÓN

Desde siempre la información que se posee de otros – y su acceso- ha constituido un bien valorado y preciado por las personas, ya que les permite tomar decisiones más eficientes respecto de una amplia gama de situaciones que van desde el ámbito estrictamente personal al profesional o comercial. Como indica Richard Posner[1], esbozando una explicación a lo señalado anteriormente, "*I believe such an explanation is possible, most clearly where an actual or potential relationship, whether business or personal, creates opportunities to profit (monetarily or not) from possessing information about someone else*". Efectivamente la información y más específicamente, una correcta y acertada información, es necesaria para la eficiente toma de decisiones de todas las personas, incluyendo las de los agentes económicos de la sociedad chilena.

En prácticamente todas las sociedades, el control y acceso a la información constituyen 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[2]. Como indica Keneth Laudon[3]. "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 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".

[1] POSNER, Richard. The Economics of Justice. Cambridge, Harvard University Press, 1981. 232p.
[2] WELLS, Anne. Who owns information. New York, Basic Books, 1994. 241p.
[3] 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.

En este último tiempo, esta demanda por información personal ha ido aumentando de la mano de la tecnología, generándose un escenario de acceso a ella más rápido y económico para quien la necesite o la solicite. Este aumento en el mercado de la información personal, ha generado que las personas se sientan ahora más amenazadas en su privacidad que antaño. Surge, así con más fuerza el conocido conflicto o choque en la protección de distintos bienes jurídicos: ¿Protegemos el derecho de las personas a mantener su información personal alejada del conocimiento de terceros, les otorgamos el derecho a decidir sobre quién y cómo se puede acceder a esa información? o bien, ¿Protegemos el derecho de las personas a conocer la información de terceros?, es decir, en una sola pregunta ¿a quién asignamos la titularidad respecto al control o decisión sobre este ámbito de la privacidad, cual es la información personal?, y, luego, ¿cómo protegemos esa titularidad?

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 por una multiplicidad de fines, por ejemplo, para efectuar marketing directo[4]. Lo descrito anteriormente genera un claro conflicto de intereses entre estos sujetos[5], 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

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

[5] 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. KANG, Jerry. 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. WELLS, Anne. op.cit. pág 3.

protección de ellas; por acuerdo entre las partes; por el mercado o, finalmente, utilizando en forma conjunta alguno de las vías mencionadas anteriormente. Uno de los objetivos de esta tesis es referirse a estos distintos métodos y descubrir cuáles de ellos nos pueden llevar a una solución eficiente en términos económicos.

Una forma interesante de examinar cómo nuestro sistema jurídico ha dado respuesta a estas interrogantes, es hacerlo desde la perspectiva del Análisis Económico del Derecho[6]. Para ello, utilizaremos los principios que entregaran en su célebre artículo los profesores Calabresi y Melamed, "Reglas de propiedad, reglas de responsabilidad y de inalienabilidad. Una Vista a la Catedral"[7], el Teorema de Coase[8] y algunos aspectos fundamentales de la teoría económica de la propiedad.[9] Como indican Kai-Lung Hui y I.P.L. Png, "la privacidad es multidisciplinaria y ha sido y debiera ser analizada desde múltiples perspectivas –derecho, psicología, sociología, ciencia política y la economía-. La economía es una disciplina especialmente apropiada desde que provee un marco para apreciar las claves de las compensaciones que existen en las políticas hacia la privacidad"[10].

Es, entonces, finalidad central del presente trabajo exponer algunas ideas respecto a la asignación de titularidades efectuada por el legislador en la Ley 19.628 y las formas en que esas titularidades se protegen en esta normativa, explorando por último, si esta asignación y vías de protección resultan adecuadas y eficientes, sosteniendo de nuestra parte la hipótesis que no lo

---

[6] "El análisis económico del derecho es una rama de la ciencia económica casi completamente incluida dentro del campo de la microeconomía. Su objetivo es analizar y evaluar el papel de las normas jurídicas dentro del funcionamiento de los mercados, a través del estudio de su impacto sobre el comportamiento de los agentes económicos y su repercusión en las cantidades y los precios. Al igual que la economía como un todo, el análisis económico del derecho tiene un enfoque positivo y un enfoque normativo. El análisis positivo busca explicar el efecto de las normas jurídicas sobre los distintos mercados y en ciertas circunstancias produce además teorías que pretenden encontrar causas económicas en la adopción de ciertas normas por parte de las distintas sociedades. El análisis normativo, en cambio, sirve para brindar prescripciones respecto de cuáles normas jurídicas son más adecuadas en una situación o en otra, según cuál sea el objetivo buscado por el legislador". COLOMA, Germán. Apuntes para el Análisis Económico del Derecho Privado Argentino, CEMA Working Papers Universidad del CEMA, 1999. 156p.

[7] CALABRESI, Guido y MELAMED, D. Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. Harvard Law Review, Vol. 85, Nº 6, 1972, pp. 1.089-1.128.

[8] El profesor Ronald H. Coase. Premio Nobel de Economía, expone este teorema en "The Problem of Social Cost", Journal of Law and Economics, vol. 3, 1960.

[9] Julie Cohen indica que dentro de la academia legal en torno al largo debate sobre la privacidad informacional, la discusión del valor y el significado social de los datos personales es crecientemente enfocado en términos económicos. COHEN, Julie. Examined Lives: Informational privacy and the subject as object. Stanford Law Review 52: 1373-1437, 2000. pág. 1403.

[10] Hui, Kai-Lung y Png, Ivan. The economics of privacy. Handbook of information systems and economics. 2005. Elsevier, Terry Hendershott ed. pág. 5.

son, de manera que se proponen finalmente, los elementos que debiera contener un nuevo modelo de protección de daos personales en nuestro ordenamiento.

Cabe señalar que la necesidad de discutir sobre estas materias es más necesaria y actual que nunca, lo que se demuestra en la cantidad de proyectos de ley que buscan modificar la normativa vigente en la materia en nuestro país, en que el gobierno está estudiando actualmente modificar esta norma, incluyendo la creación de un órgano de control en el ámbito de la protección de datos personales; y finalmente; en el hecho que la propia ciudadanía ha puesto en discusión estos temas[11].

La presente tesis se encuentra estructurada en cinco capítulos. El primero de ellos, Economía de la Información y Privacidad Informacional, tiene por objeto fundamental poner al lector en conocimiento sobre aquellos aspectos que resultarán esenciales a la hora de comprender el resto de la tesis, para ello este primer capítulo recoge las distintas miradas de diversos autores sobre el impacto que han tenido las Nuevas Tecnologías de la Información y la Comunicación sobre la información y la privacidad. Luego, dado que esta tesis busca estudiar la problemática del tratamiento de datos personales desde un punto de vista fundamentalmente económico, nos referiremos a la información y su relación con la economía, primordialmente se referenciará el concepto de bien económico, todo lo anterior desde la perspectiva de la privacidad. Sentadas estas nociones fundamentales, se ahondará en la privacidad informacional, concepto que proviene del ámbito norteamericano y que se condice con lo que en el derecho europeo y latinoamericano se conoce como autodeterminación informativa, este acápite -que es el más extenso- se referirá además al porqué es necesaria la protección de la privacidad, efectuándose un estudio pormenorizado de legislación comparada en estas materias, la que en general se fundamenta en los llamados principios del tratamiento de datos personales, los que son revisados al final del capítulo.

El segundo capítulo, Análisis de la Normativa Nacional en Materia de Protección de Datos Personales, en Especial de la Ley 19.628, contiene un estudio pormenorizado, basado en la historia de la ley, la jurisprudencia y doctrina existente en la materia, respecto del

[11] Mis datos personales sin protección. El Mercurio, Santiago, Chile, 14 oct., 2006. C-5. Mercado Información Personal. ¿Cómo sabe Ud. mis datos? El Mercurio, Santiago, Chile, 12 ago., 2006. E-4.

ordenamiento jurídico nacional en el ámbito de la protección de datos personales; fundamentalmente se estudia la Ley 19.628 haciendo hincapié en la autorización del titular de los datos para el tratamiento y en las diferentes categorías de datos personales que es posible vislumbrar en la norma referida, a partir de la mayor o menor importancia que reconoce la señalada ley a la autorización del titular, tema que resultará esencial a la hora de desarrollar los capítulos siguientes.

El tercer capítulo, Caracterización del Mercado de Datos Personales en Chile, busca presentar las principales características que reviste el mercado de datos personales en nuestro país en la actualidad. Para ello, se efectuó un estudio de la forma en que opera este mercado, cuáles son sus actores principales y qué datos son los que mayoritariamente se están comercializando, de manera que se revisa el mercado de los datos patrimoniales; con fines publicitarios o de marketing; de identificación; en Internet; de salud y públicos.

En el cuarto capítulo, Análisis Económico del Mercado de Datos Personales y su Regulación, se establecen las bases doctrinarias sobre las cuales se discutirá en el capítulo siguiente respecto a cuál es el modelo que se ha de adoptar en el mercado de datos personales; de esta manera, nos referimos en primer lugar a las razones de índole económica que explican la existencia de un mercado de datos personales; luego y reconociendo la importancia de este mercado estudiamos cuáles son las fallas que se han detectado en él, las cuales en gran medida fundamentan la necesidad de regular este mercado; en esta parte, se indican las distintas formas que se reconocen para lograr este objetivo, cuales son: el propio mercado a través fundamentalmente de la autorregulación y el estado, ya sea asignando legalmente titularidades sobre la información personal al titular de los datos o bien a aquellos que efectúan el tratamiento de la referida información; finalmente, nos preocupamos de señalar los principales argumentos en pro y en contra de la propietarización de la información personal como una forma de solucionar los problemas que se derivan de las fallas del mercado de datos personales y la falta de protección a la privacidad informacional de las personas.

En el capítulo final, Un Modelo de Propuesta, se efectúa una revisión de las críticas realizadas a la Ley 19.628, como asimismo, se establecen los diversos modelos de protección de datos personales que hemos encontrado en la doctrina. Luego de ello, elaboramos nuestro

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. Finalmente, hacemos una referencia a las críticas doctrinarias que podrían aplicar al modelo planteado.

Por último, el lector encontrará un anexo y un glosario. El primero, tiene por objeto introducir a aquellos que no se encuentren cercanos a la economía, en algunos de los temas económicos que resultan esenciales a la hora de comprender lo aquí expuesto. El glosario cumple con esta misma finalidad, sólo que su consulta resulta más específica, ya que se encuentra acotado a definir conceptos económicos que son utilizados en este trabajo.

CAPITULO PRIMERO

INFORMACION Y PRIVACIDAD INFORMACIONAL

1.1. La revolución de las Tics y su impacto en la información y la privacidad

Si estamos de acuerdo con la premisa que indica que desde siempre se ha recogido y tratado información personal[12], cabe preguntarse ¿qué hace que en nuestros tiempos la discusión sobre la protección de la privacidad informacional o de los datos personales tenga tanta importancia a nivel académico, legislativo y social en general? Anne Wells esboza una respuesta basada en la arremetida de las nuevas tecnologías de la información y la comunicación (TICs)[13], indica: "la información que se encontraba garabateada ininteligiblemente en hojas de papel en distintas partes, difícil de encontrar y recolectar, y virtualmente imposible de comparar, ahora puede ser recolectada fácilmente, leída por rayos de láser electrónicos, grabada magnéticamente en forma invisible al ojo humano, y rápidamente cruzada y comparada"[14], de esta manera casi cada cosa que hacemos parece poder ser almacenada y tratada, generando información personal transable. Las compras que se pagan con cualquier medio de pago que no sea dinero (billetes) son memorizadas y contabilizadas; los depósitos y retiros bancarios son grabados y guardados;

[12] Así lo reconoce Oscar Puccinelli, cuando señala que "Desde luego que el tratamiento de información no es un fenómeno novedoso o reciente, pues la mentada relevancia económica, social y jurídica de la información siempre ha significado para quien cuenta con ella en cantidad y calidad la oportunidad de contar con una importante cuota de poder económico y político". PUCCINELLI, Oscar. El hábeas data en indoiberoamérica. Santa Fé de Bogotá, Editorial Temis, 1999. 607p. pág. 11.

[13] Se han esbozado múltiples conceptos respecto de qué se debe entender por TICs, de nuestra parte nos guiaremos por la definición entregada por Manuel Castells, quien indica que "Entre las tecnologías de la información incluyo, como todo el mundo, el conjunto convergente de tecnologías de la microelectrónica, la informática (máquinas y software), las telecomunicaciones/televisión/radio y la optoelectrónica. Además, a diferencia de algunos analistas, también incluyo en el ámbito de las tecnologías de la información la ingeniería genética y su conjunto de desarrollos y aplicaciones en expansión". CASTELLS, Manuel. La era de la información: economía, sociedad y cultura. Madrid, Siglo veintiuno de España editores, 1999. Vol.1 pág. 56.

[14] WELLS, Anne. op. cit. pág. 3. En este mismo sentido se pronuncia Curtis Taylor, quien señala que "Las innovaciones en tecnologías de información han revolucionado muchas industrias, de hecho, han creado nuevos mercados para nuevos bienes y servicios mientras al mismo tiempo crea nuevas preguntas en relación a políticas públicas. La pregunta principal se relaciona con el impacto de la revolución en tecnologías de información en la privacidad personal, especialmente, el debate envuelve derechos sobre la recolección, almacenamiento, y venta de los datos personales tales como historias crediticias individuales, datos médicos o criminales". TAYLOR, Curtis. 2004. Privacy and information acquisition in competitive markets. [en línea] <http://www.econ.duke.edu/Papers/Other/Taylor/privacy.pdf> [consulta: 18 junio 2005]. pág. 1.

las visitas al doctor, diagnósticos, prescripciones, son encriptadas y transferidas; todo lo que se visita en Internet es apuntado y retenido. Una variedad de empresas recolectan información personal, como nivel de rentas, intereses, historia de empleos, salud, compras y preferencias. Toda esta información es recolectada, reunida y almacenada en computadores. Cualquier persona que tenga una razón para ello, puede confrontar la información personal almacenada en un computador con la información almacenada en cualquier otro computador. El reporte que resulta de lo anterior puede ser usado, vendido, publicado o confrontado con otras fuentes de datos personales[15].

Como señalábamos, las TICs han generado un nuevo escenario que permite y facilita el tratamiento de datos personales a gran escala y bajos costos, lo anterior puede ser analizado desde un punto de vista económico y también desde la privacidad. Como indica Anne Wells, la nueva velocidad y exactitud de los métodos de recolección y cruce de información han dado valor económico a información que antes no lo tenía, creando nuevos intereses de propiedad y una tensión entre la necesidad de fomentar nuevas tecnologías basada en el comercio de la información y la necesidad de determinar cuál será una conducta social responsable en la sociedad de la información[16].

Respecto del primer punto de vista, es decir, el enfoque económico Richard Posner[17], entrega una interesante visión de la interacción entre las TICs y la economía, de una parte, y su efecto en la privacidad, por otra. Señala este autor que el progreso tecnológico ha aumentado los ingresos medios en la mayoría de las naciones, pero que también se debe considerar, la posibilidad que la tecnología pueda amenazar la libertad de las personas por su efecto en la privacidad. Respecto de lo anteriormente dicho, se pronuncia sobre los dos aspectos principales de la privacidad: la soledad y el secreto. La soledad –que no es sinónimo de aislamiento, sino de poseer suficiente espacio privado para permitir a una persona pensar en ella misma- fomenta las actitudes individualistas. El secreto, de su parte, en el sentido de la ocultación de lo que uno piensa, escribe, hace o dice a amigos u otros, envuelve un pensamiento y planificación en orden

[15] LITMAN, Jessica. Information privacy/information property. Stanford Law Review 52: 1283-1313, 2000.
[16] WELLS, Anne. op. cit. pág. 3
[17] POSNER, Richard. 1999. Orwell versus Huxley: Economics, Technology, Privacy and Satire. John M.Olin Law & Economics Working Paper. The Law School University of Chicago. (89): 1-35. pág 8.

a mantenerse escondido de las autoridades. De este modo, según Posner, la soledad crea las condiciones elementales para un pensamiento independiente, y el secreto crea las condiciones esenciales para el refinamiento y la propagación de lo que se pensó. Efectuando un análisis de los conocidos libros Un Mundo Feliz de Huxley y 1984 de Orwell señala que en ambos se pueden observar los altos costos sociales de un régimen que proteja la privacidad, en el cual los avances tecnológicos hacen que sea costoso mantener la privacidad resultando dramáticamente menos privacidad en las sociedades que exponen los referidos libros comparada con nuestra actual sociedad.

Richard Posner considera a la privacidad como soledad y como secreto, como un bien económico, y su demanda y oferta condiciones a ser investigadas e indica que ambas, y sobre todo, la privacidad como soledad pueden ser consideradas como un bien superior en un sentido económico: la demanda de ellas crece con el incremento del ingreso. De su parte, el precio de oferta varía por muchos factores económicos, en el caso de la privacidad como secreto, que es especialmente la que nos interesa, el precio de oferta sube con la rápida expansión del almacenamiento y recuperación de datos computarizados y especialmente, por la existencia de Internet; es crecientemente costoso mantener secreta cualquier información que se encuentra grabada, ya sea un registro médico, registros de compras, o documentos de propiedad. Puesto lo anterior de otra manera, Posner indica que el costo de invadir la privacidad ha disminuido con la llegada de la "revolución de la información" (TICs), sin embargo, es improbable que la cantidad neta de privacidad haya disminuido, desde que es un bien superior y desde que la gente hoy en día está mejor informada, es más individualista y más asertiva que en el pasado, por lo cual es posible esperar que la privacidad, en balance, haya crecido.

Compartimos la conclusión de Richard Posner, pero establecemos como requisito esencial para afirmar que la privacidad ha crecido, el que justamente estemos en presencia de una sociedad informada, que en el ámbito de los datos personales, se traduce en que los titulares de dichos datos, tengan conocimiento respecto de qué datos personales suyos son tratados, quién los trata, con qué finalidad, y si estos datos son cedidos a terceros. Resulta fácil concluir que este requisito no se encuentra presente en sociedades como la nuestra, en la cual no obstante existir

---

Richard Posner es considerado en la actualidad como un referente fundamental en el análisis económico del derecho.

una ley especial que regula la protección de los datos personales[18], la sociedad en general no se encuentra informada respecto de los puntos señalados anteriormente. Tal vez la única excepción, se encuentra en el tratamiento de datos personales patrimoniales que efectúan ciertas empresas privadas como por ejemplo, Dicom-Equifax[19]. Lo anterior se explica, porque el tratamiento de datos que efectúa la referida empresa es masivo, y porque la existencia en las bases de datos personales de Dicom-Equifax de datos personales patrimoniales negativos o positivos respecto del comportamiento de una determinada persona no la deja indiferente, ya que de ello puede por ejemplo, depender la obtención de un crédito o un empleo.

Asimismo y por otra parte, son varios los autores que dan cuenta de los efectos negativos de las tecnologías de la información sobre los derechos del hombre, y en particular sobre la privacidad, incluso algunos han señalado que "la revolución de la información tiene un lado oscuro, debido a que existe una pérdida de privacidad"[20]. En este mismo sentido, Miguel Angel Davara[21] con una mirada un tanto catastrófica indica: "Alrededor de las Tics, está girando un cambio social; un interesante y beneficioso cambio social; pero un instrumento tecnológico tan útil puede convertirse en una herramienta peligrosa. Para evitarlo es preciso que el progreso de la técnica, que tantas ventajas aporta, fuera acompañado de una mayor profundización en determinados principios éticos y de defensa a ultranza de los más elementales derechos del hombre. Sin ellos la sociedad podría llegar a disponer de instrumentos cada vez más sofisticados, pero humanamente sería insoportable".

Curtis Taylor[22], ya desde un análisis económico, reconoce los efectos de los importantes avances en la adquisición tecnológica de la información los cuales han generado costos y

[18] Ley 19.628. CHILE. Ley sobre Protección de la vida privada. Santiago, Chile, 28 de agosto de 1999.
[19] Lo anterior se encuentra demostrado en la investigación "Intimidad y nuevas tecnologías. Análisis de la tutela efectiva a los derechos de los titulares de datos personales en Chile". Concurso de Ciencias Sociales, Humanidades y Educación DID 2002 de la Universidad de Chile. En la referida investigación, se confirmó a través de un estudio de las sentencias de los Tribunales de Justicia, que la gran mayoría de acciones judiciales intentadas por los titulares de datos en orden a defender su privacidad por el tratamiento indebido de sus datos personales, se dirigió en contra de la empresa señalada, asimismo, mediante una encuesta telefónica se demostró el casi total desconocimiento que tiene el ciudadano medio chileno acerca de los derechos que le asisten respecto del tratamiento de sus datos personales.
[20] THEORY OF TRANSACTIONS PRIVACY. Por CHARLES KAHN "et al". Federal Reserve Bank of Atlanta, Working Paper Series. 2000-22. 27p.
[21] DAVARA, Miguel Angel. De las autopistas de la información a la sociedad virtual. Pamplona, Editorial Aranzadi S.A., 1996. 191p. pág. 14.
[22] TAYLOR, Curtis. op.cit. pág.1.

beneficios sociales. Los beneficios se derivan principalmente por la mayor eficiencia producida por la mejor asignación de bienes, servicios y puestos de trabajo. De este modo, contratos de seguro, de crédito, de trabajo y otros pueden ser adaptados mejorando la información de los posibles consumidores. Existen, sin embargo, dos costos asociados con el aumento en la adquisición de información, derivado de las nuevas tecnologías. Primero, el costo directo obvio relacionado con la recolección, almacenamiento y procesamiento de los datos. Segundo, existe un costo en términos de la privacidad personal. Específicamente, mientras consumidores y/o futuros empleados están dispuestos a divulgar su información personal en orden a obtener términos contractuales más favorables, las empresas tienen menos probabilidad de recolectar el nivel eficiente de información sobre los consumidores y/o futuros empleados, ya que generalmente adquirirán de éstos más información personal que la cantidad eficiente de ella, lo que nos lleva a concluir que existe una renuncia a la privacidad por parte de los titulares de datos, que no resulta eficiente desde un punto de vista económico.

Antonio Pérez-Luño[23], ya desde un punto de vista más garantístico, evoca estas mismas ideas, haciendo presente la posibilidad de vigilancia continua e inadvertida del ciudadano que se halla fichado en un banco de datos, que lo afecta potencialmente incluso en los aspectos más sensibles de su vida privada. Señala como ejemplos de lo anterior, "el control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro y gestión de las adquisiciones comerciales realizadas con tarjetas de crédito, así como las reservas de viaje…"

Por último y a modo de corolario en esta parte, cabe señalar que el cambio fundamental que existe en nuestro días en el ámbito de la privacidad, como señala Mercedes Galán[24], es que sus fronteras, que estaban constituidas por el elemento temporal y espacial, hoy en día dada la tecnología y la informática han desaparecido, "el tiempo facilitaba, con su transcurso, que se diluyeran los recuerdos de las actividades ajenas, impidiendo, así la configuración de una historia lineal e ininterrumpida de la persona. El espacio, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de hechos

[23] PÉREZ-LUÑO, Antonio. Intimidad y protección de datos personales: del habeas corpus al habeas data. EN: Estudios sobre el derecho a la intimidad. Madrid, Editorial Tecnos. 1992. pp. 36-45. pág 38.

protagonizados por los demás, que hubieran tenido lugar lejos de donde nos hallamos". Hoy en día, el mercado de la información y la tecnología han llevado a que aquello que no se quiera olvidar, no sea olvidado, y que aquello que se quiera conocer, sea conocido, no importando cuánto tiempo o dónde haya pasado.

1.2. Información y economía. La información como bien

La información y la economía se encuentran relacionadas en distintos e importantes aspectos, es así como la información constituye un factor relevante al momento de establecer supuestos en un determinado modelo económico, como sucede, por ejemplo, en la existencia de mercados de competencia perfecta, ya que si no hubiese información perfecta entre los agentes que participan en el mercado no se lograría un equilibrio competitivo y eficiente. De otra parte, la posesión de información por solo uno de los agentes en una determinada transacción, es tratada en la ciencia económica como una falla de mercado, la denominada asimetría de información[25]. Dentro de las múltiples relaciones existentes entre los conceptos mencionados, de las cuales sólo se han expuesto aquí algunas, centraremos nuestro estudio en este primer acápite en la información como bien económico, es decir, como un objeto que posee valor en el mercado y que, por lo tanto, es transado.[26]

Iniciaremos este acápite definiendo la información en relación a su propiedad económica en la sociedad, para luego establecer las diversas relaciones que mantiene con el concepto de privacidad de los agentes económicos, concluyendo con una referencia a la información como bien, particularmente, como bien público.

1.2.1. Información y sociedad.

En primer lugar resulta indispensable dar respuesta a la pregunta: ¿qué entendemos por información? El primer escollo que encontramos es que la palabra información es un concepto polisémico, es decir, que presenta una pluralidad de significados, lo que nos lleva a detectar cuál

---

[24] GALÁN, Mercedes. Intimidad. Nuevas dimensiones de un viejo derecho. Madrid, Editorial Centro de Estudios Ramón Areces S.A., 2005. 278p. pág. 205.
[25] Para una definición de los conceptos económicos utilizados en esta tesis, ver el glosario.
[26] Algunos de estos tópicos se encuentran explicados con mayor profundidad en el anexo de esta tesis

de esos distintos significados en particular, es el que aplica a nuestro estudio. El Diccionario de la Lengua Española de la Real Academia Española [27] ofrece varias definiciones del concepto al cual nos referimos, entre las que podemos destacar "acción y efecto de informar", "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada" y "conocimientos así comunicados o adquiridos"[28]. En otras palabras, la información puede ser conceptualizada como lo "que" se comunica, el acto de comunicar o el resultado de la comunicación siendo uno de sus objetivos primordiales el obtener un determinado conocimiento, es decir, saber sobre algo o alguien. La referencia a la relación entre información y dato, es de utilidad al momento de dar contenido al significado de la información. De la señalada vinculación entre estos conceptos, que es con bastante ocurrencia indicada en textos sobre la materia, cabe referirse a la opinión de dos autores; M. Porat[29], para quien la información son los datos que se han organizado y comunicado y L. Thayer[30], quien indica que los procesos de comunicación organizan y convierten los datos propiamente dichos en unidades de información, y que es precisamente la información, no los datos, lo que constituye la materia prima del pensamiento, la decisión y el aprendizaje.

Para nuestros propósitos, entenderemos a la información como cualquier antecedente o dato que pueda ser utilizado por los agentes de la economía para generar conocimiento y hablaremos de información personal, cuando este conocimiento versa sobre las personas y su comportamiento.

Ya desde otra perspectiva y tomando como base los principios generales de la economía, podemos afirmar que, en general, la existencia de información para la economía y la sociedad es más beneficiosa que su ausencia, ya que genera conocimiento, lo cual ayuda a las personas a tomar decisiones informadas, y consecuentemente, más eficientes.

'Generalidades del análisis económico del derecho y de la teoría económica de la propiedad'.

[27] Diccionario de la Lengua Española de la Real Academia Española. 2001. Vigésimo segunda edición.

[28] Gonzalo Abril, hace notar el carácter polisémico del concepto de información, al señalar que "Cuando se examinan las acepciones de la voz "información", en el Diccionario de la Lengua de la RAE, se advierte que sólo dos de ellas, (la séptima y la octava) aparecen bajo el epígrafe comunicación, y que además, conciernen genéricamente al conocimiento, a su adquisición y ampliación. Hay también acepciones pedagógicas, biológicas, jurídicas y por supuesto, comunes." ABRIL, Gonzalo. Teoría general de la información. Madrid, Ediciones Cátedra S.A. 1997. 344p. pág. 15.

[29] PORAT, Marc. The information economy: definitions and measurement. OT Special Publication 77-12 (1), US Department Of. Commerce. 1997. pág. 2.

[30] THAYER, Lee. Comunicación y sistemas de comunicación. Barcelona, Península. 1975. pág. 52.

Lo señalado en el párrafo anterior explica en gran medida, a nuestro entender, la irrupción en la última década de los tan ya conocidos conceptos de sociedad de la información, sociedad informacional y sociedad del conocimiento, los cuales han sido esbozados por varios autores con el objeto de ilustrar la importancia que la información y el conocimiento que genera, tienen en nuestra sociedad actual. Muchas definiciones se han esbozado de estos términos, tomaremos las efectuadas por Manuel Castells[31], quien distingue entre la sociedad de la información[32] y la sociedad informacional, señalando que "El término sociedad de la información destaca el papel de esta última en la sociedad. Pero yo sostengo que la información, en su sentido más amplio, es decir, como comunicación del conocimiento ha sido fundamental en todas las sociedades…En contraste, el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de la productividad y el poder, debido a las nuevas condiciones tecnológicas que surgen en este período histórico". De lo señalado por Manuel Castells, se manifiesta cómo la información en la actualidad, toma más que nunca, un cariz esencialmente económico, ya que constituye una fuente generadora de productividad y poder. Por otra parte, este mismo autor indica que la sociedad del conocimiento "se trata de una sociedad en la que las condiciones de generación de conocimiento y de procesamiento de información han sido sustancialmente alteradas por una revolución tecnológica centrada en el procesamiento de información, la generación del conocimiento y las tecnologías de la

[31] CASTELLS, Manuel. La era de la información: economía, sociedad y cultura. Madrid, Siglo veintiuno de España editores. 1999. Vol.1. pág. 47. Manuel Castells es uno de los autores que más ha estudiado este tema y constituye una autoridad reconocida en estos ámbitos. Ente otras definiciones de la sociedad de la información encontramos la de Philip Elliot, quien indica que ésta se refiere a la sociedad postindustrial caracterizada por un rápido cambio tecnológico y por los desarrollos consiguientes de la electrónica, de los sistemas de procesamiento de información y de nuevos *media*. ELLIOT, Philip. Intellectuals, the "information society" and the disappearence of the public sphere. 1986. pág. 109. De su parte, Yoneji Masuda, quien es uno de los primeros en utilizar el término, se refiera a la sociedad de la información como aquella que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad humana, en lugar de un aumento del consumo material". MASUDA, Yoneji. La sociedad informatizada como sociedad post-industrial. Madrid, Tecnos. 1984. 171p.

[32] Manuel Castells define la sociedad de la información como un nuevo sistema tecnológico, económico y social. Una economía en donde el incremento de la productividad no depende del aumento cuantitativo de los factores de producción (capital, trabajo, recursos naturales), sino de la aplicación de conocimientos e información a la gestión, producción y distribución, tanto en los procesos como en los productos. CASTELLS, Manuel. op. cit.

información"[33], como podemos observar en la definición de sociedad del conocimiento, se pierde la relevancia que en la sociedad informacional, tiene el elemento económico.

Para Gonzalo Abril[34], la información ha adquirido en la sociedad actual un carácter complejo, debido al papel fundamental de aquélla como proceso y recurso estratégico, y por la creciente mundialización de la economía y el mercado. A partir de ello, divide la sociedad en tres clases, en su relación con la información, a saber: la sociedad informacional, que se caracteriza por la forma en que los medios tecnológicos tratan hoy al lenguaje y al conocimiento y pueden transmitirlo a distancia; la sociedad informada, que lo es tal fundamentalmente debido a la existencia de la sociedad informacional, y, por último, la sociedad informativa, cuyo aspecto central es el discurso informativo, a través de noticias, conocimiento, y datos (nuevos modos discursivos derivados del procesamiento informático).

Es posible afirmar que los países desarrollados se encuentran en una sociedad informacional representada por organizaciones inteligentes, ciudadanos informados y un sector de la información emergente. Como indica Diego Cardona[35], estos países han visto disminuir la participación de su sector industrial en el Producto Interno Bruto en comparación con el sector de servicios, como consecuencia de la progresiva transformación de la sociedad industrial en una sociedad de la información. Transformación que se expresa en que la competitividad, la eficacia y la supervivencia de las empresas en el mercado, depende crecientemente de la gestión inteligente de sus activos de información. De este modo, los ciudadanos están cada vez más y mejores informados, puesto que utilizan las tecnologías de la información y consumen grandes cantidades de información en el ocio y en el trabajo. Todo lo anterior se debe gracias a la creación de un sector de la información constituido por tres grandes segmentos. El primero de ellos es el de la industria de los contenidos, el cual está formado por todas las organizaciones que generan propiedad intelectual, es decir, los contenidos que serán utilizados por organizaciones y ciudadanos gracias a los instrumentos de proceso y manejo de información. El segundo es el de la industria de la distribución y del acceso a la información constituido por las empresas que

[33] CASTELLS, Manuel. 2002. La dimensión cultural de Internet. [en línea] <http://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.htm> [consulta: 25 junio 2005]. pág. 2

[34] ABRIL, Gonzalo. Teoría general de la información. Madrid, Ediciones Cátedra S.A. 1997. 344p. pág. 33.

crean y gestionan redes de comunicación que permiten el acceso a la información. Por último, se encuentra el segmento de la industria telemática, la cual fabrica el hardware y software necesarios para el procesamiento de información.

En relación con lo expuesto, resulta interesante reseñar a uno de los autores más citados en materia de economía de la información, Marc Porat[36] quien en el año 1977, estableció una categorización de la economía a partir de la información en Estados Unidos, indicando que existían dos sectores distinguibles en la economía, el primario y el secundario; dentro del primero se encuentran aquellas industrias que usan su información en mercados establecidos o en cualquier otro lugar en el cual sea fácilmente posible otorgar un valor económico a esa información; el secundario, en cambio, dice relación con actividades de investigación, creación de información para organismos gubernamentales, bibliotecas, etc. A partir de lo anterior, este autor concluyó, ya en esa época, que el 46% de la población norteamericana estaba de alguna manera vinculada con el sector de la información, constituyendo, consecuentemente la norteamericana una economía basada en la información y como tal, una sociedad donde las mayores y principales áreas de la actividad económica son aquellas que producen bienes y servicios de información.

El anterior escenario también es reconocido por actores del ámbito del derecho, José María Alvarez Cienfuegos[37] indica: "La información, de la índole que sea, se ha convertido en un bien jurídico de extraordinario valor. No sólo mueve intereses económicos importantes sino que, también, constituye un elemento imprescindible para el desarrollo de múltiples iniciativas públicas y privadas". Es por lo anterior, señala con mucha razón, que resulta difícil una política que limite o condicione el acceso a la información… mucha de ella de carácter personal.

Concluimos entonces y en resumen, que el cambio en la generación, procesamiento, y divulgación de la información, con la ayuda de las nuevas tecnologías, ha producido cambios fundamentales en la sociedad actual, dentro de los cuales, a nuestros efectos, uno de los más

---

[35] CARDONA, Diego. 2002. Economía o sociedad de la información. [en línea] <http://dsi.esade.edu/dcardona/CV/publicac.htm> [consulta: 05 junio 2005]. pág. 1.

[36] PORAT, Marc. op. cit. Ver además, FLORES, Antonio. Sociedad de la información. [en línea] <http://www.monografias.com/trabajos15/sociedad-informac/sociedad-informac.shtml> [consulta: 30 septiembre 2005].

importantes es el mayor valor que, desde un punto de vista económico, se le entrega hoy a la información.

1.2.2. Información personal y privacidad

Ya claro el concepto de información e información personal que utilizaremos en esta tesis y la importancia de éstas en la sociedad actual, nos avocaremos ahora a comprender el significado que adopta la privacidad en su relación con la información personal.

Por una parte, existe consenso en que es relevante para toda persona tener control y tomar conocimiento sobre la información que se tenga registrada en bases de datos públicas y privadas sobre ella, ya que esto implica –junto con otros medidas- asegurar cierto nivel de privacidad para tal persona, al poder ésta saber quién, cómo y de qué manera se trata su información personal, ya que este conocimiento le permitirá, si así lo desea, reaccionar en caso que su privacidad u otros derechos se estén vulnerando por el tratamiento de su información personal. Para aquellos que adscriben a lo anteriormente expuesto, la información personal que es seleccionada, elaborada, procesada y probablemente destinada a la venta, debería encontrar ciertas restricciones cuando afecta los ámbitos de la privacidad de las personas, sobre todo, cuando el desarrollo de las nuevas tecnologías, hace cada vez más ágil y veloz los intercambios de esta información, por lo tanto, ponen a la privacidad de las personas en riesgo, en caso que los datos personales reciban un tratamiento contrario a los derechos humanos, o bien, ellos sean un instrumento para fines ilícitos y todo tipo de actividades que afecten la libertad de las personas, contrarias a las prácticas democráticas y de respeto a las libertades individuales[38].

De otra parte, existen cuestionamientos respecto al planteamiento anterior, basados en que la privacidad y otros derechos fundamentales, constituyen una barrera tanto de entrada como de salida de información que puede resultar necesaria para la toma de decisiones eficientes para

---

[37] ALVAREZ-CIENFUEGOS, José María. La defensa de la intimidad de los ciudadanos y la tecnología informática. Pamplona, Editorial Aranzadi S.A. 1999. 161p. pág. 13.
[38] ARENAS, María. 2002. Nuevas tecnologías y sistemas de información: contextos y paradigmas. [en línea] < http://www.redcom.org/CCC/foro6_arenas.htm> [consulta: 05 junio 2005]. pág. 8.

los agentes económicos[39]. Asimismo, se critica que la privacidad protege la conducta antisocial, es decir, se utiliza para esconder las actividades que se deben desalentar o desincentivar. Una tercera crítica se basa en que la privacidad es costosa para la economía, en otras palabras, que la protección de la privacidad aumenta el costo de búsqueda de información, el engaño llega a ser más fácil y, por lo tanto, los costos de transacción suben[40].

Como se puede observar la relación entre información y privacidad no es pacífica, presentándose dos grupos de opinión claramente diferenciados respecto a cuál de ambas debe primar por sobre la otra. De nuestra parte, constituirá uno de los objetivos de esta tesis tratar de esbozar una conclusión respecto de cuál es el punto de equilibrio eficiente entre ambas, en relación con la protección de datos personales.

1.2.3. La información como bien económico

En general, al referirnos a los bienes estamos implícitamente refiriéndonos a objetos tangibles o intangibles que son provechosos ya que entregan cierto nivel de utilidad o bienestar a quienes los consumen. Específicamente, los bienes económicos se producen para que exista un intercambio de ellos en el mercado, por lo tanto, podríamos denominarlos mercancías que entregan satisfacción directa o indirectamente a las necesidades de los consumidores. Sin embargo, para que esta mercancía u objeto sea considerado en su totalidad un bien económico, debe poseer cierta demanda por parte del mercado, provocando la existencia de agentes que estén dispuestos a pagar debido a que cumple con la capacidad de satisfacer sus necesidades.

Al estudiar, entonces, los intercambios en la economía podemos observar que la información ha pasado a ser en la actualidad un bien económico muy preciado en nuestra sociedad para todos los agentes del mercado. De hecho, hoy en día, las demandas por información son cada vez mayores ya que ella es visualizada por los productores como un insumo productivo que les entrega valor agregado en el proceso de producción de bienes o servicios. Lo anterior, permite plantear que la información ha pasado a ser un recurso de real

[39] El ejemplo más común de conflicto entre la información y la privacidad, se produce cuando las empresas tratan y difunden información sobre la capacidad de las personas para satisfacer sus deudas para el otorgamiento de créditos.

importancia al momento de evaluar proyectos de inversión por parte de las firmas y, por lo tanto, en su toma de decisiones.

Una de las características económicas más importantes de la información es que la misma información puede ser utilizada de diferentes maneras por diferentes personas, como señala Miguel Angel Davara[41], "es un bien que no se agota con su consumo y que puede ser utilizado por muchas personas al mismo tiempo, sin que por ello se cause ningún daño o perjuicio al propio bien que, posiblemente, sea favorable a múltiples intereses distintos para los que se produjo", lo anterior, se explica porque una vez que los costos iniciales de generar y "producir" la información se contraen, los usos adicionales se pueden emprender a un costo marginal relativamente bajo. De hecho, publicistas, instituciones financieras y compañías de seguros pueden usar la misma información comercial y cooperar en su generación, aun cuando cabe señalar que si bien estos actores utilizan la misma información, la naturaleza del uso es bastante distinta. De este modo, podemos concluir que la información ha ido asumiendo cada vez más, la particularidad de ser un bien económico ya que presenta las cualidades de poder entregar riqueza a sus productores, por medio de su uso como materia prima en el proceso productivo. Incluso, esta nueva definición de la información ha provocado que sea transada de múltiples maneras para poder obtener beneficios en distintos ámbitos de la economía. En particular, generando nuevas formas de procesar e intercambiar los datos personales registrados en bancos de datos.

En este orden de ideas es claro que la información sobre las personas o datos personales, constituye también un bien económico. A este respecto cabe preguntarse cuál es la naturaleza de esta información, desde un punto de vista económico, esto es, si se trata de un bien privado o público.

La definición de bien público (puro) contempla, por una parte, la no rivalidad en el consumo. Un ejemplo convencional de un bien de esta naturaleza es el alumbrado público. El

---

[40] NOAM, Eli. Privacy and self-regulation: Markets for electronic privacy. [en línea] <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm> [consulta: 12 febrero 2005]. pág. 3

[41] DAVARA, Miguel. op.cit. pág. 50. Señala este autor, además, que la no agotabilidad de la información permite que su expansión se haya producido no sólo a través de una mayor creación de información sino en gran medida provocada por el desarrollo alcanzado en los sistemas de

hecho de proveer a un individuo la luz en una calle no disminuye la cantidad de luz que se ofrezca a otros individuos. Pero existe, además, otra característica que posee un bien público. Una vez que se definen los derechos de propiedad sobre los bienes privados resulta relativamente fácil que el dueño de los derechos pueda excluir a otros del uso de tales bienes a un costo bajo. Sin embargo, en el caso de los bienes públicos, resulta costoso excluir a cualquiera. De hecho, resulta imposible ofrecer cantidades diferentes de luz pública. La primera condición -el no tener rivalidad- permite que el mercado pueda asegurar la provisión del bien. En efecto, esta propiedad solamente especifica que no es posible racionalizar su uso, es decir, que para obtener sus beneficios no es necesario competir por ellos, ya que todos los individuos de una sociedad se benefician. Asimismo, cuando no es posible aplicar la segunda condición podemos encontrar que el mercado falla debido a que al participar en el consumo no es necesario realizar un pago directo, con lo cual los individuos no están obligados a revelar sus preferencias ni ofrecer precios por los bienes públicos. De este modo, si el bien fuera producido por el mercado existirían individuos que se comportarían como "*free riders*" quienes no pagan su consumo del bien público y, por lo tanto, no se generaría una cantidad eficiente en el sentido de *Pareto*, es decir, asignaciones de recursos que tienen la propiedad de no poder mejorar el bienestar de ninguna persona sin empeorar el de otra.

Las propiedades económicas de rivalidad y exclusión son útiles para examinar la naturaleza de la información y en particular, la de los datos personales. Como el uso o la posesión de los datos personales por una de las partes no impide su uso o posesión por otros, los datos personales son no-rivales, lo que hace que constituyan un bien público. Sin embargo, determinar si uno puede excluir a otros de utilizar o compartir los datos personales una vez que se reúnen, es más problemático. Aquellos que señalan que esa información debe ser libre y accesible a todos, ven a este bien, o sea, los datos personales como no-excluibles y no-rivales (bien público puro), lo que se evidenciaría en el libre comercio de los datos personales en el mercado secundario[42] y en las débiles demandas por la no asignación de derechos de

telecomunicación que han permitido que una misma información sea accesible a un mayor número de usuarios.

[42] A estos efectos entendemos como mercado secundario a aquél en que los datos personales son transados por agentes o sujetos que no han obtenido una autorización directa del titular de los datos para efectuar tal tratamiento, es decir, se trata de tratamiento de datos personales que han sido cedidos por el responsable del banco de datos originario.

propiedad.[43]

Tabla 1

Rivalidad, Exclusión y Derechos de Propiedad

	Exclusión	No exclusión
Rival	Bienes Privados	Bienes Cuasi-Públicos
No Rival	Bienes Cuasi-Privados	Bienes Públicos Puros
Derechos de Propiedad	Individuales	Colectivos

Con respecto a lo último, un punto importante es cómo asignar eficientemente los derechos de propiedad ya que de este modo podemos solucionar las fallas de mercado debido a que los datos personales pasarían a constituir un bien "cuasi-privado" en el cual la exclusión es posible (véase Tabla 1). Efectivamente, según Ellen Rose[44] los derechos de propiedad en la propiedad intangible (los datos personales poseen una propiedad intangible debido a que no es un bien físico) se refieren a la "habilidad de controlar o restringir el acceso a manifestaciones físicas de mis datos personales", y por lo tanto, poder con este instrumento – esto es, con la asignación de derechos de propiedad- solucionar las distorsiones generadas en el mercado de la información[45].

[43] ROSE, Ellen. Data users versus data subjects: Are consumers willing to pay for property rights to personal information? Proceedings of the 38th Annual Hawaii International Conference On System Sciences. 2005. pág. 2.
[44] Ibid.
[45] Volveremos a este punto en el Capítulo IV de esta tesis.

1.3. La privacidad informacional

1.3.1. Nociones previas

Antes de analizar lo que denominamos en esta tesis como privacidad informacional[46] y que usualmente en el ámbito nacional y europeo se conoce como autodeterminación informativa o libertad informática[47], efectuaremos ciertas delimitaciones terminológicas en torno a la intimidad y la privacidad, conceptos utilizados cuando se habla del fundamento último del derecho que se analiza[48].

La intimidad es reconocida como un derecho relativamente nuevo: la gran mayoría de los autores citan el artículo que escribieran Warren y Brandeis en 1890 en la *Harvard Law Review*, denominado "*The right to privacy*" como el hito decisivo en el surgimiento del concepto de intimidad. Estos autores reconocieron a la intimidad como el derecho a ser dejado solo, el derecho a la soledad, "*the right to be left alone*". A partir de esta idea, se han escrito numerosos textos que tratan de definir el concepto de intimidad. Así por ejemplo, para Luis García San Miguel[49], la intimidad es el derecho a no ser conocidos, en ciertos aspectos, por los demás; es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos. En este mismo sentido, Alfredo Chirino[50] partiendo de la base que la intimidad es un bien jurídico que se reduce a la esfera más privada y recóndita del ser humano, señala que "resulta ser la intimidad un

[46] Traducción del concepto esencialmente norteamericano *Informational privacy*.
[47] A estos términos es posible agregar dos más: el de protección de datos personales y de hábeas data. Para un estudio acabado respecto de los diversos términos utilizados por la doctrina para este nuevo derecho ver JAÑA, Washington. Análisis legal comparativo de la protección de datos personales a nivel latinoamericano. (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Facultad de Derecho, Universidad de Chile. 2003. 516h.
[48] Todavía cabría referirse a la conceptualización del derecho a la vida privada, que por lo demás es el que utiliza nuestra Constitución Política, sin embargo, creemos que con ello nos excederíamos de nuestro objetivo. Basta a este respecto señalar, que nuevamente observamos que distintos autores utilizan el concepto de vida privada como sinónimo de intimidad, así por ejemplo, Eduardo Novoa señala: "El llamado derecho a la vida privada surge de manera específica en los Estados Unidos, en 1890, al aparecer el estudio de Warren y Brandeis titulado *The right of privacy*. Poco antes el juez norteamericano Cooley había proclamado el derecho a ser dejado tranquilo y de no ser arrastrado a la publicidad, como lo propio del derecho a la intimidad". NOVOA, Eduardo. Derecho a la vida privada y libertad de información. Un conflicto de derechos. 5ª ed. México, Siglo veintiuno editores. 1979. 224p. pág. 26.
[49] GARCÍA, Luis. Reflexiones sobre la intimidad como límite de la libertad de expresión. EN: Estudios sobre el derecho a la intimidad. Madrid, Editorial Tecnos. 1992. pp. 15-35. pág 18.
[50] HASSEMER, Winfried. y CHIRINO, Alfredo. El derecho a la autodeterminación informativa y los restos del procesamiento automatizado de datos personales. Buenos Aires, Editores del Puerto s.r.l. 1997. 238p. pág. 89.

derecho subjetivo de defensa frente a otros seres humanos y frente al Estado, a fin de impedir un ingreso no deseado en esa esfera donde se desarrollan los elementos más característicos de la individualidad humana: como sus creencias, sus convicciones y opiniones políticas, su libertad sexual y religiosa, etc." Este aspecto negativo del derecho a la intimidad que se refleja en la definiciones recién indicadas, ha evolucionado adoptando actualmente también un aspecto positivo, como indica Ana Herrán[51] "el derecho a la intimidad aparece configurado como un derecho de doble perspectiva, una negativa, propia de los derechos subjetivos, que se traduce en el poder de exclusión del conocimiento ajeno de aquello que se refiere a la propia persona, y una perspectiva positiva, de control y vigilancia por el interesado de la información que le afecta". Este aspecto positivo de la intimidad, fue reconocido ya en la década del 70 por dos autores norteamericanos: Fried en 1979 en un trabajo que lleva el nombre de *An anatomy of values,* quien define a la intimidad como el control sobre la información que nos concierne y Parker, en trabajo de 1974, con el título de *A definition of privacy*, que la define como el control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona[52].

Interesante resulta la conceptualización social de la intimidad efectuada por Antonio Pérez-Luño[53], que se aleja del concepto individualista del ser dejado solo tanto en su aspecto negativo como positivo, al señalar que "la intimidad en la pluralidad de sus acepciones, se halla en directa e insoslayable relación con otros valores (dignidad, libertad, libre desarrollo de la personalidad, autodeterminación...); que tales valores no constituyen categorías axiológicas cerradas y estáticas, pues cuando más se profundiza en el significado de cada uno de ellos más evidente resulta su interdependencia con los demás, y que la intimidad, lejos de implicar autoconfinamiento del sujeto moral, supone su incorporación a un proceso de estímulos y proyecciones sociales".

Ya respecto de la relación que existe entre la intimidad y la privacidad compartimos el criterio de aquellos que ven entre ambos conceptos una diferencia de intensidad y, por lo mismo,

---

[51] HERRÁN, Ana. El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales. Madrid, Dykinson. 2002. 388 p. pág. 25.
[52] El trabajo de Parker, A definition of privacy, está recogido en la antología de textos publicados por LEISER, Burton. Values in conflict, liberty and the rule of law, New York Mac. Millan. 1981. La definición de Fried viene recogida por el mismo Parker en aquel trabajo. cit. por GARCÍA, Luis. op. cit., pág. 17.
[53] PÉREZ-LUÑO, Antonio. op.cit. pág. 39.

de amplitud[54]. A este respecto Francisco González señala que "En el sistema jurídico del *common law*, el término *privacy* es extraordinariamente amplio, siendo muy difícil determinar con exactitud su núcleo de significado… el término intimidad, en cambio, es mucho más acotado y preciso que el de privacidad, y se refiere específicamente al ámbito de lo reservado, lo secreto, lo íntimo, del cual se puede excluir a terceros"[55]. De su parte, Mercedes Galán señala que "las nociones de intimidad y *privacy* coinciden en sus elementos básicos aunque la diferencia entre ambas es de grado: mientras que la primera se refiere a ámbitos de secreto y retiro que pertenecen al espacio más espiritual de la persona, con predominio de la dimensión física, con la que se identifica la propia persona, la segunda lo hace en ámbitos de retiro y de secreto que no tienen por qué ser en absoluto espirituales o íntimos, poniendo por ello el énfasis en el hecho de estar apartado de los demás"[56]. En el mismo sentido, Miguel Angel Davara señala, "el derecho que se trata de proteger no es solamente el de la intimidad, sino algo con mayor profundidad que, en los ordenamientos de ámbito anglosajón, se ha dado en llamar *privacy* y que nosotros hemos españolizado como privacidad"[57].

Cabe consignar que para algunos esta distinción entre los conceptos de intimidad y privacidad, ya se encuentra superada, en el ámbito de la protección de datos personales, e incluso

[54] Esta idea se encontraba recogida en la exposición de motivos de la ley española de protección de datos personales (LORTAD) que fuera derogada por la LOPD, se indicaba: "Nótese que se habla de privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de las personas –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado". De otra parte, existen una serie de autores, que hacen sinónimos ambos términos, así v.gr. Marc Carrillo señala "El derecho a no ser molestado o el derecho a estar solo (*to be left alone*) es una expresión que ha hecho fortuna para describir el derecho de la persona a proteger su vida privada y su intimidad. Formulada en estos términos, el derecho a la intimidad, a la *privacy*, según la expresión anglosajona, responde a un planteamiento que es propio del liberalismo clásico". CARRILLO, Marc. El derecho a no ser molestado. Información y vida privada. 2003. Navarra, Aranzadi. 172p. Asimismo, lo indican Losano, Pérez-Luño y Guerrero: "La historia del derecho a la intimidad, o *privacy*, es una historia típicamente anglo-americana". Libertad informática y leyes de protección de datos personales. 1989. Por MARIO LOSANO "et al". Madrid, Centro de Estudios Constitucionales. 213p. En este sentido, Joaquín Bayo señala "La protección de datos, concebida en su momento inicial como un aspecto de la intimidad (lo que en inglés se conoce como "privacy") fue incorporada al elenco de derechos fundamentales en los instrumentos internacionales correspondientes". BAYO, Joaquín. Derecho comunitario sobre protección de datos. EN: GOMEZ, M. Derecho a la intimidad y nuevas tecnologías. Madrid, Consejo General del Poder Judicial. 2004. pp. 45-76.

[55] GONZÁLEZ, Francisco. 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. 154.

[56] GALÁN, Mercedes. Intimidad. Nuevas dimensiones de un viejo derecho. Madrid, Editorial Centro de Estudios Ramón Areces S.A. 2005. 278p. pág. 24.

[57] DAVARA, Miguel Angel. La protección de datos en Europa. Principios, derechos y procedimiento. 1998. Madrid, Grupo Asnef Equifax. 204 p. pág. 19.

resulta artificial e inútil, a este respecto Ana Herrán[58] indica "intimidad y privacidad no constituyen sino dos aspectos complementarios e interdependientes de la existencia humana, quiere ello decir que una protección completa de la persona frente a las agresiones de las tecnologías de la información únicamente se alcanzará a través de la tutela de ambas esferas de actuación de la persona". En este mismo sentido se pronuncia Osvaldo Gozaíni[59], para quien la intimidad y la privacidad no son realidades contrastables en el ámbito de la protección de datos personales, explicándose indica: "La *privacy* se concibe por un sector doctrinal como una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona que, si bien ha emergido al exterior, fuera de la esfera íntima de la persona, y se han incorporado a un archivo electrónico nada impide que puedan continuar bajo control y salvaguarda de su titular".

Por último, cabe señalar como precisión terminológica que en esta tesis utilizaremos el vocablo privacidad en vez de intimidad, vida privada, derecho al honor, u otros semejantes, debido a que gran parte de la bibliografía utilizada para aquellos capítulos que se refieren a este derecho de los individuos es norteamericana y, asimismo, en reconocimiento de los hechos que muestran que la palabra privacidad ya se encuentra incorporada a nuestra realidad[60], pero por sobre todo, porque la protección de datos personales abarca ámbitos más amplios que la sola intimidad, los cuales se acercan más al concepto de privacidad.

1.3.2. Clasificaciones de privacidad.

La dificultad de definir la privacidad es reconocida por casi la totalidad de los autores que han escrito sobre el tema y que han sido consultados para la realización de esta tesis; como señala Jerry Kang "la privacidad es un camaleón que cambia su significado dependiendo del contexto"[61]. Dado lo anterior, es útil referirse al contenido y significado de la privacidad no en forma unívoca, sino que reconociendo sus múltiples facetas, a través de las clasificaciones que de ella han efectuado algunos autores.

---

[58] HERRÁN, Ana. op.cit. pág. 44.
[59] GOZAINI, Osvaldo. Hábeas data. Protección de datos personales. Doctrina y jurisprudencia. Buenos Aires, Rubinzal-Culzoni. 2001. 526p pág. 84.
[60] La vigésimo segunda edición del año 2001 del Diccionario de la Real Academia de la Lengua Española ha incorporado el concepto de privacidad, definiéndola como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Jerry Kang divide a la privacidad en tres categorías: espacio, decisión e información[62]. La primera categoría, se refiere al espacio físico del individuo, en particular, la extensión en la cual el territorio del individuo se encuentra protegido de invasiones no deseadas de objetos o señales, es el sentido de la privacidad empleado cuando uno se queja del ruido de las alarmas de los autos. La segunda categoría que vislumbra este autor –privacidad decisional- se relaciona con la capacidad de elección; con la capacidad del individuo de tomar decisiones significativas sin interferencia, se refiere a la toma de decisiones relativas, por ejemplo, a matrimonio, procreación, métodos anticonceptivos, relaciones familiares, educación de los niños, etc.[63] Como tercera categoría, menciona este autor a la privacidad informacional, como aquella que se refiere al control del individuo sobre el procesamiento -adquisición, divulgación y uso- de su información personal. Así, esta categoría de privacidad es invadida cuando alguien obtiene datos médicos sensibles de archivos confidenciales sin autorización[64].

Por último, este autor señala que estas categorías pueden converger y estar simultáneamente implicadas en una situación determinada, como por ejemplo, en los casos de llamadas telefónicas de telemarketing o los correos no solicitados, en donde se ven involucradas tanto la privacidad entendida como soledad como, asimismo, la privacidad informacional.

Richard Posner[65] también efectúa una clasificación tripartita de la privacidad, ya que señala que ésta posee tres distintos significados: secreto, retiro y autonomía. Nos referiremos en forma separada y con alguna profundidad, a cada uno de estos significados.

Para este autor, la privacidad como secreto significa mantener oculta información, particularmente información personal[66]. Planteándose a este respecto una esencial pregunta: la cuestión si y hasta qué punto las personas deben tener un derecho legalmente protegido para

---

[61] KANG, Jerry. op.cit. pág. 1202.
[62] Ibid.
[63] Esta concepción de la privacidad es claramente estadounidense. Los temas que menciona Jerry Kang han sido llevados a los tribunales de justicia, por los ciudadanos norteamericanos invocando la vulneración de derechos constitucionales.
[64] Con todo, este autor reconoce que existen serios argumentos en orden a señalar que estas tres categorías que él reconoce de privacidad, puede ser integradas en un solo valor moral como la dignidad humana o la inviolabilidad de la personalidad. KANG, Jerry. op. cit. pág. 1204.
[65] POSNER, Richard. The economics of justice. Cambridge, Harvard University Press. 1981. 415p.
[66] POSNER, Richard. op.cit. pág. 231.

ocultar información personal sólo porque algunas personas quieren descubrir tal información. La segunda pregunta que efectúa Posner es por qué las personas quieren descubrir tal información. ¿Es un asunto puramente de curiosidad, o es funcional, esto es, económica, la explicación? Para este autor la explicación es de naturaleza económica, sobre todo, allí donde existe una relación actual o potencial, sea de negocios o personal, ya que en este tipo de relaciones se crea la oportunidad de obtener beneficios, ya sean monetarios o no, en el hecho de poseer información acerca de otra persona[67]. Asimismo, los individuos demandan información personal de otros como una forma de auto-protección[68]. Ya dando respuesta a la primera cuestión planteada, Posner señala que no es claro el porqué la sociedad debe asignar el derecho a la propiedad de la información personal al individuo a quien pertenece, desde su punto de vista es incorrecto e ineficiente si la ley permite a un vendedor pregonar sus artículos haciendo representaciones falsas o incompletas de su calidad, asimismo, sería ineficiente si se le permitiera a las personas encubrir o mantener secreta cierta información sobre ellas, ya que "las personas se "venden" así como sus bienes profesando altos estándares de conducta para inducir a terceros a negociar con ellas, ya sea en el ámbito social o de negocios, mientras que encubren los hechos que los terceros necesitan para evaluar su carácter"[69].

El segundo significado de privacidad para Posner, es el retiro, que se configuró en el siglo XVII como el alejamiento de la vida pública a través de la mudanza a lugares apartados. Su característica principal es la reducción de la interacción social. Asimila esta categoría al "derecho a ser dejado solo" en el sentido expuesto por Warren y Brandeis, pero, efectúa una distinción, ya que señala que esta categoría de privacidad abarca a lo menos dos tipos de intereses: Uno es el interés de ser dejado solo, interés que es invadido por las llamadas telefónicas no solicitadas, ruidos molestos, música en los elevadores, ser empujado en la calle, etc. Este interés es invadido, incluso, si el invasor no lo busca y no obtiene ninguna información, privada o de otra clase del individuo cuya paz y tranquilidad es invadida. El segundo interés,

[67] Richard Posner indica: "Esto es lo que motiva la demanda de información personal por el recaudador de contribuciones, por el prometido, por el socio, por el acreedor, y por el competidor. Menos obvio resulta el fisgoneo o curiosidad casual (el término es usado aquí sin connotación peyorativa) en la vida privada de colegas, de amigos, tan característica de la vida social, sin embargo, también este fisgoneo puede ser motivado por consideraciones racionales de interés. Fisgonear le permite a uno formar un retrato más exacto de un amigo o un colega, y el conocimiento ganado es útil en el trato social o profesional con él. Por ejemplo, en la elección de un amigo, uno quiere saber si él será discreto o indiscreto, egoísta o generoso, y estas calidades no son siempre patentes en el trato inicial". POSNER, Richard. op.cit. pág. 232.
[68] POSNER, Richard. op.cit. pág. 238.

ocultamiento de la información, es invadido cada vez que información privada es obtenida en contra de la voluntad de la persona a la cual pertenece la información. Si la invasión perjudica o no la paz y quietud del individuo es irrelevante, sin embargo, el conocimiento que esa información ha sido o será comunicada puede alterar dicha paz y quietud. Lo anterior, concluye este autor, implica señalar que las personas valúan más la privacidad como secreto que la privacidad en el sentido de ser dejado solo o retiro[70].

Por último, Posner señala que la privacidad también significa -para algunos- autonomía o libertad. Esta categoría describe el interés de ser autorizado a hacer lo que se quiera hacer sin interferencia. Este autor critica la consideración de la privacidad como autonomía, ya que a su entender, ya existen conceptos como libertad y autonomía que definen esta idea.

Alfredo Bullard[71] reconociendo la simplicidad de su clasificación, divide la problemática de la privacidad en dos aspectos: el derecho a estar solo y el derecho a que cierta información no sea revelada.

El derecho a estar solo es entendido por este autor como el derecho a mantener un espacio (temporal y físico) libre de la intromisión de los demás. Es pues, indica, la posibilidad de excluir a los otros de estar en algún lugar y en algún momento en que uno no desea que estén. Da como ejemplos típicos: la intimidad del hogar, la posibilidad de no ser visto desnudo, de conversar por teléfono libre de intervenciones o interferencias ajenas, el poder ir a un restaurante o a un hotel sin tener que preocuparse de que los periodistas le sigan o le tomen fotografías, etc. Bullard enfoca el derecho a estar solo a partir de la teoría económica de los derechos de propiedad, es decir, propietariza este tipo de privacidad, según este autor "De la misma manera como no es posible que exista un mercado de automóviles sin que existan derechos de propiedad sobre los mismos, no es posible que exista una capacidad de disponer del propio tiempo y la posibilidad de excluir a los terceros de un espacio físico, si no se reconociera la privacidad como un derecho de los particulares. El reforzamiento de este derecho da a nuestro tiempo y espacio

[69] POSNER, Richard. op.cit. pág. 233.
[70] POSNER, Richard. op.cit. pág. 272.
[71] BULLARD, Alfredo. No se lo digas a nadie. Se puede vender el derecho a la privacidad en el mercado. EN: Revista Ius et Veritas. 1998. (17).

valor económico"[72]. Así, esta concepción de este aspecto de la privacidad, permite que ésta sea considerada como una institución económicamente eficiente y que maximiza el bienestar existente en nuestra sociedad y permitiendo un mejor uso de los recursos escasos. Dentro de esta acepción la privacidad no sólo no entra en contradicción con el mercado, sino que es un derecho plenamente consistente para el desarrollo del mismo. Es la forma como se incorpora al mercado el tiempo y el espacio controlado por las personas, eliminando la existencia de bienes públicos sobre dicho espacio o tiempo, y con ello dando coherencia al reconocimiento de la privacidad dentro del mercado[73]. Por último, en esta parte, resulta muy interesante la reflexión que efectúa este autor cuando considera a la privacidad como generadora de un bienestar individual que refleja el valor del uso "bien" privacidad, este bienestar será socialmente eficiente si los beneficios que genera son mayores a los que generaría a terceros el poder acceder al espacio privado de la persona. Esa persona puede escoger entre ambas alternativas, es decir entre vender su privacidad o mantener el uso privado de ella. El hecho que no la venda refleja que el mercado no ha generado un precio que le brinde un bienestar mayor al que le da el uso exclusivo de su espacio privado. Ello demuestra que el uso privado es socialmente más eficiente que la invasión pública a dicho espacio, como el hecho que uno viva en su casa y no la venda refleja que el valor de uso para el titular se encuentra por encima del valor de mercado de la misma. Si la privacidad no existiera el valor de ese uso privado sería una pérdida de eficiencia económica[74].

El segundo tipo de privacidad que reconoce este autor es aquella a la que denomina el derecho a que cierta información no sea revelada, categoría que buscaría proteger el uso y difusión de información de una persona sobre lo que hizo, lo que fue o lo que es, sin perjuicio de que su obtención no requiera afectar la "soledad" de las personas[75]. El análisis económico que efectúa este autor respecto a este segundo tipo de privacidad es diametralmente distinto del que revisáramos a propósito del derecho a estar solo, ya que cuestiona la eficiencia de establecer reglas de privacidad y las consecuentes asignaciones de derechos, debido a que su entender esta información personal "es especialmente relevante para la toma de decisiones de terceros que podrían ser ineficientes o inadecuadas (o simplemente equivocadas) si es que no está a

[72] BULLARD, Alfredo. op.cit. pág. 9.
[73] BULLARD, Alfredo. op.cit. pág. 13.
[74] BULLARD, Alfredo. op.cit. pág. 16.
[75] BULLARD, Alfredo. op.cit. pág. 18.

disposición de tales terceros"[76], de manera que el tema de la información disponible para la toma de decisiones adecuadas puede entonces entrar en contradicción con la idea de proteger la esfera privada. La pregunta que surge entonces es cómo establecer un límite razonable entre ambas necesidades (la de información frente a la generada por la privacidad).

Albert J. Marsella y Carol Stucki[77], presentan una clasificación de la privacidad un tanto distinta de las anteriores y conforme a las diversas dimensiones que posee según estos autores, así distinguen entre: privacidad de la persona *"bodily privacy"* que dice relación con la integridad del cuerpo del individuo, incluyendo tópicos como inmunización obligatoria, transfusión de sangre sin consentimiento, esterilización obligatoria, entre otros; privacidad de la conducta personal *"media privacy"* que dice relación con todos los aspectos de la conducta, pero especialmente materias sensibles, como las preferencias sexuales o hábitos, actividades políticas y religiosas, tanto en lugares públicos como privados; privacidad de las comunicaciones personales *"intercepction privacy"* que implica que los individuos puedan comunicarse con otros, sin ser monitoreados por otras personas u organizaciones; y finalmente, la privacidad de los datos personales *"informational privacy"* o *"data privacy"* que dice relación con las demandas de los individuos en orden a que sus datos personales no sean automáticamente disponibles para otros individuos u organizaciones, y que, aun cuando otra persona los posea, el individuo tenga la capacidad de ejercer un control sustancial sobre esos datos y su uso.

De nuestra parte, creemos que partiendo del reconocimiento que la privacidad tiene un solo fundamento cual es la autonomía y dignidad humana, es posible reconocer una clasificación bipartita de la privacidad; de una parte, el derecho de toda persona a conservar fuera del conocimiento de terceros aquella información que desea se mantenga en ese estado, que llamamos privacidad informacional, y de otra parte, el derecho de todo ser humano a no ser invadido en aquellos espacios o ámbitos que considera propios y exclusivos, como su casa, correspondencia, su cuerpo, imagen, etc., que llamaremos privacidad espacial. En la presente tesis se tratará en profundidad la privacidad informacional.

[76] Ibídem.

1.3.3. Del porqué de la protección a la privacidad.

Porqué buscamos la privacidad es una pregunta cuya respuesta es de mucha utilidad a los efectos de este estudio, ya que determina la razón por la cual la sociedad y el derecho en tanto elemento regulador de ella, han ideado modelos, herramientas, normas cuyo objetivo es asegurar la privacidad en sus múltiples acepciones. A este respecto, Jerry Kang[78] menciona cuáles son los propósitos de la privacidad. El primer fin que menciona es el de evitar la vergüenza o incomodidad. Este sentimiento ha estado presente desde antaño en todas las culturas, en donde la divulgación de ciertas conductas, acciones o hechos resultan vergonzosos para el individuo. El segundo, se refiere a la construcción de la intimidad, debido a la capacidad del individuo de revelar su información personal selectivamente. Y por último, la privacidad busca evitar malos usos, específicamente la privacidad protege en contra de usos impropios de la información personal, siendo esta última razón aquella que nos ha de interesar en esta tesis[79]. Según este autor, los datos personales pueden ser mal usados en dos instancias: la primera, cuando ciertas decisiones que dicen relación con los titulares de datos son tomadas en base a información personal de poca calidad[80] y la segunda, cuando el mal uso de información personal hace a los individuos vulnerables a actos ilícitos y malas prácticas. En nuestro ámbito múltiples son los casos que han llegado a nuestro conocimiento sobre tratamiento de datos personales de mala calidad; personas que se les ha rechazado un cheque por estar en calidad de moroso en el sistema de morosidad de Dicom-Equifax debido al no pago de un cuota del "Tag" en la autopista central, en circunstancias que esa persona no posee automóvil, o bien, el tratamiento de los datos de salud por empresas, que efectúan tratamiento de datos respecto de las compras efectuadas con receta médica o a partir del cruce de información que se efectúa cada vez que damos nuestro número de cédula de identidad al momento de comprar en alguna farmacia.

---

[77] MARCELLA, Albert y STUCKI, Carol. Privacy Handbook. Guidelines, exposures, policy implementation and international issues. New Jersey, John Wiley & Sons, Inc. 2003. 357p. pág. 53.

[78] KANG, Jerry. op. cit. pág. 1212.

[79] Respecto de la sentencia de Jerry Kang, sólo una observación: la privacidad protege de usos impropios o malos usos de la información personal, pero no de aquellos que resultan lícitos y adecuados.

[80] Indica este autor que una de las maneras de evitar esta información de mala o baja calidad, es entregarle al titular de los datos mayor control sobre el flujo de su información personal, ya que un individuo con este control tomará medidas preventivas, como por ejemplo, mantener los datos personales irrelevantes fuera del alcance de aquellos que toman las decisiones. KANG, Jerry. op. cit. pág. 1214.

Para Stan Karas[81], una de las razones más importantes por la cual se debe restringir la recolección de información personal es que esta práctica menosprecia la dignidad del individuo. Señala que para aquellos que sostienen este punto de vista, la privacidad es un derecho humano fundamental, una característica propia de la personalidad, de manera que el tratamiento de datos es moral y éticamente incorrecto. Esta tesis sostiene que la protección de la privacidad es una condición socialmente deseable para el desarrollo de la personalidad. Sobre lo anterior, este mismo autor señala algunos problemas en emplear la dignidad como fundamento de protección de la información personal[82] en primer lugar, indica que este argumento es muy rígido en su enfoque respecto al control sobre los datos personales; en segundo lugar, carece de la necesaria apreciación acerca de las significantes diferencias en el contexto social y cultural de los diferentes tipos de tratamiento de datos; en tercer lugar, es contradictorio con las prácticas existentes en materia de tratamiento de datos; y, por último, no es viable en esta sociedad contemporánea en donde los individuos generan enormes cantidades de información diariamente.

Algunos explican la necesidad de protección de la privacidad desde un punto de vista esencialmente económico, así, por ejemplo se ha dicho que "Uno podría pensar que no existe "demanda por la privacidad", sin embargo, existe un gran número de consumidores que estarían dispuestos a pagar para aumentar su privacidad. Con que más de la mitad de la población esté dispuesta a pagar, es imposible que la privacidad no sea un tema relevante a tratar**"[83].**

En el ámbito europeo también se reconoce la necesidad de regular el tratamiento de datos en un libre mercado, efectuando asimismo, un reconocimiento a la importancia que reviste este mercado desde la eficiencia. Lo anterior, se ve reflejado en lo que señala Peter Harris quien es *Data protection commissioner of Bailiwik of Guernsey*, "La economía del mercado libre depende de la competencia para manejar bajos precios, pero necesita la regulación adecuada para asegurar justicia en el comercio y protección al consumidor. La regulación del procesamiento de datos personales interviene en el libre mercado haciendo cumplir los derechos de los individuos

[81] KARAS, Stan. 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] pr. 50.
[82] Si bien este autor efectúa estas críticas en el marco de la información personal de los consumidores, creemos, que igualmente puedes aplicarse en forma amplia a todo tipo de información personal.

e imponiendo estándares a los que efectúan tratamiento de datos, por lo tanto, no es sorprendente que cualquiera que regule el procesamiento de datos personales requiera proporcionar una justificación económica para su existencia. En Europa, la regulación ha tendido a desarrollarse por poderes reglamentarios concedidos en funcionarios públicos independientes, mientras que en otras partes del mundo puede haber habido una tendencia a alentar la autorregulación. Generalmente, se piensa que la protección de datos es una "cosa buena", pero hay muy pocos datos disponibles en relación a los costos de aplicar una política de regulación de la privacidad e incluso menos sobre sus beneficios económicos. Los beneficios de una fuerte regulación son en su mayor parte intangibles, pero contribuyen a una creación de una sociedad justa y abierta. La pregunta que queda ¿son los costos equilibrados por los beneficios?"[84]

En el ámbito nacional, Iñigo de la Maza[85] refiriéndose específicamente a la privacidad en el ámbito de Internet, justifica la protección de la privacidad desde un punto de vista económico, señalando que "la falta de protección a la privacidad de los usuarios representa el costo de oportunidad en que incurren los usuarios cada vez que navegan en la red. Lo anterior implica que, al menos, aquellos individuos que representen aversión al riesgo poseerán fuertes incentivos para no revelar información personal en la red y, eventualmente –si resulta factible vincular hábitos en la red con personas reales- no utilizar la red para temas que desearían explorar protegidos por el aura de la privacidad. Aun en actores que se comporten con neutralidad al riesgo, la falta de certeza respecto de la protección de la información que ellos mismos consideran como confidencial o que no desearían se divulgase se incorpora como un costo al momento de utilizar la Red."

En el entendido que la presente tesis trata de analizar la problemática en estudio desde el análisis económico del derecho y reconociendo que en la actualidad ya existe un gran mercado de datos personales, tanto en nuestro país como a nivel mundial, postulamos que una de las razones más fuertes para proteger la privacidad es el resguardo de la calidad de tales datos, esto es, en términos simples, que el dato refleje en forma exacta la realidad de la cual pretende dar

---

[83] NOAM, Eli. op.cit.
[84] HARRIS, Peter. The european perspective: is data protection value for money? [en línea] <http://26konferencja.giodo.gov.pl/data/resources/HarrisR_paper.pdf> [consulta: 19 marzo 2006]. pág. 1.

cuenta. En este escenario, la protección de la privacidad se lograría asignando la titularidad del derecho a los sujetos a los cuales les pertenece la información, ya que son éstos o -a lo menos en teoría debieran serlo- los primeros en tener conocimiento de los cambios que se producen respecto de la información que les concierne, siendo ellos, en consecuencia, los que al tener el control sobre su información, aseguren en buena medida que los datos personales que se encuentran en el mercado sean datos de calidad, es decir, sean exactos y reflejen realmente la realidad[86].

1.3.4. Concepto

Ante la necesidad de proteger los intereses de los individuos en orden a controlar la información que terceros poseen de ellos, es que surge la autodeterminación informativa, libertad informática[87] o privacidad informacional. Como revisáramos unos parágrafos atrás, este derecho está íntimamente vinculado con la privacidad, que constituye su fin último de protección, si bien no el único, ya que es de aquellos derechos que se caracterizan por ser instrumentales, ya que a través de su reconocimiento, una serie de otros derechos y bienes jurídicos, se ven protegidos, así por ejemplo: el derecho a desarrollar una libre actividad económica, la igualdad ante la ley, la libertad de trabajo, el derecho de propiedad, etc.[88]

La Sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983, sobre la Ley del Censo de Población, es citada por la gran mayoría de los autores consultados como el hito fundamental en la afirmación del derecho a la autodeterminación informativa[89].

---

[85] DE LA MAZA, Iñigo. Privacidad y comercio electrónico. EN: DE LA MAZA, Iñigo. Derecho y tecnologías de la información. 2002. Fundación Fernando Fueyo Laneri. Escuela de Derecho. Universidad Diego Portales. pp. 265-279.

[86] Volveremos con mayor profundidad sobre este punto en el capítulo IV de esta tesis. En él se tratará el modelo que se debe construir para que los sujetos tengan los incentivos necesarios para mantener la calidad de los datos personales que le conciernen, tanto en escenarios de su conveniencia, por ejemplo cuando han pagado un crédito moroso, como en aquellos casos en que a lo menos superficialmente se pudiera pensar que es de su conveniencia mantener el dato inexacto, como por ejemplo si se informa que su patrimonio es mayor al real.

[87] PEREZ-LUÑO, Antonio. Manual de informática y derecho. 1996. Barcelona, Ariel Derecho. 222p. A estos términos utilizados por Pérez-Luño, aun se deben agregar dos: el de protección de datos personales y hábeas data, este último utilizado más propiamente para referirse a la herramienta de naturaleza procesal que tiene por objeto buscar la tutela efectiva de la privacidad informacional.

[88] Comprueba lo señalado, la gran cantidad de recursos de protección que son conocidos por nuestros tribunales de justicia que alegan la existencia de un tratamiento de datos indebido o ilegítimo vulnerador de las garantías constitucionales señaladas.

[89] Ver GALÁN, Mercedes. op.cit. pág. 208; PUCCINELLI, Oscar. El hábeas data en indoiberoamérica. 1999. Santa Fé de Bogotá, Editorial Temis. 607p. pág. 74; HASSEMER, Wifried y CHIRINO, Alfredo. op.cit. pág. 33; HERRÁN, Ana. op.cit. pág. 64, entre otros. Asimismo, quedó constancia en la

Este Tribunal resolvió un recurso presentado en contra de una ley de fecha 25 de marzo de 1982, relativa al censo demográfico; declarándola inconstitucional, en razón del excesivo número de datos o informaciones solicitadas a los ciudadanos con el fin de ser sometidos a un posterior tratamiento informático, en concreto el agravio consistía en el riesgo de la posible combinación de datos y su adscripción a una determinada persona[90]. Esta sentencia configura el derecho a la autodeterminación informativa señalando: "la facultad del individuo, derivada de la idea de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué limites procede revelar situaciones referentes a la propia vida…este derecho fundamental garantiza, en efecto, la facultad del individuo de decidir por sí solo sobre la difusión y utilización de sus datos personales".

La doctrina (fundamentalmente española y latinoamericana)[91], de su parte, está relativamente conteste en el contenido del derecho al cual nos referimos, no obstante, ser llamado por los autores de distinta forma. Emilio Suñé[92], identifica la estrecha relación existente entre intimidad y autodeterminación informativa, al indicar que ésta es una forma de referirse a las particulares características que adquiere el derecho a la intimidad en la era informática. Antonio Pérez-Luño utiliza el término de libertad informática, señalando que ésta aparece como un nuevo derecho de autotutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico. Para Mercedes Galán[93], se trata de un derecho a controlar el uso de los datos insertos en un programa computacional (*habeas data*); que comprende entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención. Ana Herrán[94] indica que el derecho a la autodeterminación informativa se identifica con la libre capacidad de decisión que todo individuo ostenta respecto de la difusión, utilización y cesión de la información que le concierne. Miguel Angel Davara[95]

---

historia de la ley 19.628, la importancia de la sentencia del Tribunal Constitucional Alemán. Cf. Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, 3er Trámite, DSS, Sesión 18ª (anexo de documentos), p. 2089.

[90] GALÁN, Mercedes. op.cit. pág. 208.

[91] Respecto de la doctrina norteamericana, ya revisamos en el acápite sobre la clasificación de la privacidad el concepto de privacidad informacional suscrito por los autores norteamericanos.

[92] SUÑÉ, Emilio. Tratado de Derecho Informático. Introducción y protección de datos personales. 2000. Madrid, Servicio publicaciones facultad de derecho Universidad Complutense de Madrid. Vol.1. pág. 29.

[93] GALÁN, Mercedes. op.cit. pág. 223.

[94] HERRÁN, Ana. op.cit. pág. 68

[95] DAVARA, Miguel Angel. op.cit pág. 17.

indica, utilizando el concepto de protección de datos y efectuando una conceptualización más acabada que las ya revisadas, que se trata aquí de la protección jurídica de las personas en lo que concierne al tratamiento automatizado de sus datos personales, o, expresado de forma más extensa, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para confeccionar una información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad. Por último, Oscar Puccinelli[96] utilizando el concepto de derecho a la protección de datos personales indica que se entiende la suma de los principios, derechos y garantías establecidos en favor de las personas que pudieren verse perjudicadas por el tratamiento de los datos nominativos a ellas referidos.

De nuestra parte, y utilizando la noción de privacidad informacional, entendemos a ésta como la facultad privativa de todo sujeto para controlar el tratamiento que de su información personal efectúan terceros, a través del ejercicio de una serie de derechos subjetivos como la autorización para el tratamiento, el acceso a sus datos personales, su eliminación o modificación, entre otros.

1.3.5. La información personal o dato personal

La información personal o dato personal[97], constituye el núcleo esencial del concepto de privacidad informacional o protección de datos personales, ya que éste se erige como un modelo de protección que poseen los individuos frente al tratamiento que -justamente- de su información personal o datos personales realizan terceros. Por ello, es importante saber de qué hablamos cuando nos referimos a éstos.

---

[96] PUCCINELLI, Oscar. op.cit. pág. 68.

[97] Si bien es cierto que los conceptos de información y dato, se encuentran relacionados, pues ambos hacen referencia a algo o alguien, son antológicamente distintos, ya que el dato constituye una representación de un hecho, un antecedente o noticia respecto de algo, en cambio, la información es el significado que toman los datos de acuerdo con convenciones vinculadas a estos datos, es la interconexión de esos datos, de manera que, vinculados, se conviertan en una referencia concreta. Dado que en el ámbito del tratamiento de datos personales, en la gran mayoría de los casos nos encontramos en un escenario de interconexión de datos, en donde el dato como entidad independiente no es considerado, hemos optado por tratar en esta tesis los conceptos de datos personales e información personal, como sinónimos. Ver sobre este tema, PUCCINELLI, Oscar. op.cit. pág. 106; DAVARA, Miguel Angel. op.cit. pág. 15; GOZAINI, Osvaldo. op.cit. pág. 113.

En general, las leyes sobre protección de datos personales, han definido a éstos en términos bastante amplios, entendiendo por tales a cualquier información respecto o concerniente a una persona a lo menos determinable. Esta amplitud del concepto permite cumplir con varios objetivos: facilita su adaptación a la constante evolución de la tecnología y la informática, utilizando el principio de neutralidad tecnológica; no limita el concepto solamente a información escrita, sino que también la imagen, la voz, las huellas digitales constituyen datos personales; y, el concepto admite "hacer frente a uno de los peligros de la informática: la acumulación de datos personales y un ulterior cruce de los mismos; entrelazamiento que permite conocer, a partir de datos personales intrascendentes de una o varias personas, particularidades que pertenecen al ámbito protegido por el derecho a la intimidad"[98].

En el ámbito de la legislación comparada, la Directiva Europea sobre la materia[99], ha dado la pauta[100] respecto a qué se entiende por datos personales, señalando en su artículo 2 letra a), que este tipo de datos es "toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social." Del concepto cabe distinguir la exclusión que se efectúa respecto de los datos de personas jurídicas, las cuales quedan fuera, por lo tanto, de protección respecto del uso que terceros pueden efectuar de la información que les concierne, lo anterior fundamentalmente porque se trata de proteger un derecho humano -la privacidad- y porque se entiende que existen otras vías legislativas especiales para proteger la información de las personas jurídicas (secreto, reserva, confidencialidad). Sin embargo, legislaciones como la de Austria, Dinamarca, Islandia, Luxemburgo, Noruega y Suiza, y Argentina han optado por ampliar el concepto de datos personales, incluyendo aquellos que se refieren a personas jurídicas. También del concepto legal de la Directiva, es dable destacar que para que estemos en presencia de un dato personal es necesario que la persona a la cual se refiere el dato sea a lo

[98] GRIMALT, Pedro. La responsabilidad civil en el tratamiento automatizado de datos personales. 1999. Granada, Editorial Comares. 382p. pág. 46.
[99] UNION EUROPEA. 1995. Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Octubre 1995.
[100] Esta Directiva es la fuente legislativa directa de todas las legislaciones protectoras de datos de los países miembros de la Unión Europea, las que se han debido adecuar a la referida directiva.

menos identificable, es decir, que la identidad de esta persona pueda ser determinable, se pueda saber, en términos simples, quién es. Lo anterior, nos lleva a concluir que aquellos datos que no se pueden identificar o asociar con una persona determinada no son datos personales. Cuando el dato no es personal, no se producen, a lo menos inicialmente problemas de privacidad, ya que el referido dato no es y no puede ser asociado a una persona identificada o identificable. A este respecto, Jerry Kang[101] señala tres situaciones en que el dato no reviste el carácter de personal: a) cuando la información simplemente no es sobre un ser humano; b) cuando la información si bien se refiere a un ser humano, es anónima. Esto es, no puede ser asociada a un individuo en específico[102]; y c) cuando la información es directamente identificable a un grupo y sólo indirectamente identificable a los individuos que componen ese grupo.

En Estados Unidos[103] no existe una legislación orgánica que establezca reglas para el tratamiento de datos personales, sin embargo, sí existe alguna legislación sectorial de la cual podemos extraer la noción de información personal. *The Cable Communications Policy Act*[104] si bien no define el concepto en forma positiva, indica qué no se debe entender por "*personally identifiable information*", señalando que se excluyen los registros de datos que no identifican personas determinadas. *The Video Privacy Protection Act*[105], define el concepto en forma positiva, al señalar que "*personally identifiable information"* incluye información que identifica a una persona que ha requerido u obtenido materiales específicos de video o servicios de un prestador de servicios de video. De la referida legislación, queda claro que la noción de información personal, "describe la relación existente entre la información y una persona, siendo esa información -sensible o no- de alguna manera identificable a un sujeto"[106].

Asimismo, aparece como fuente de las distintas leyes de protección de datos que se han dictado en Latinoamérica, incluyendo Chile y otras partes del mundo.

[101] KANG, Jerry. op. cit. pág. 1208.

[102] Este tipo de información es la que nuestra ley de protección a la vida privada define como dato disociado.

[103] El análisis de la legislación norteamericana en la materia se verá más adelante en este capítulo.

[104] ESTADOS UNIDOS. 1984. The Cable Communications Policy Act. U.S.C. 551 (1994).

[105] ESTADOS UNIDOS. 1984. The Video Privacy Protection Act. U.S.C. 551 (1994).

[106] KANG, Jerry. op. cit. pág. 1207. Este autor indica que desde su punto de vista la información puede ser *"identifiable to an individual"* en tres hipótesis: a) en una relación de autoría con el individuo, como por ejemplo, las conversaciones telefónicas, las comunicaciones escritas, un diario de vida; b) en una relación descriptiva con el individuo, como por ejemplo, información biométrica (huellas digitales, iris, ADN) biográfica (fecha nacimiento, domicilio, historia crediticia), etc.; y c) en una relación instrumental de ubicación del individuo, como por ejemplo, la cédula nacional de identidad, las claves de acceso, etc.

De lo señalado queda claro que los requisitos *sine qua non* para que estemos en presencia de información de naturaleza personal, son:

a) La existencia de una persona natural (o jurídica en algunos ordenamientos),
b) Que esa persona sea a lo menos identificable.
c) Que la información se refiera justamente a esa persona, esto es, pueda ser asociada a ella.

1.3.5.1. Clasificación

A continuación efectuaremos una clasificación de los datos personales desde los principales puntos de vista, en el entendido que no se abarcará la gran cantidad de clasificaciones que pueden efectuarse.

a) A partir de su fuente. Datos personales directos e indirectos.

Denominamos datos personales directos a aquellos cuya fuente u origen es la voluntad de su titular, ha sido éste quien ha entregado cierta información que le concierne en forma directa y voluntaria. Son indirectos, por el contrario, aquellos datos personales cuya fuente ya no es el titular de la información, sino que han sido recolectados o extraídos de o desde otros bancos de datos, a partir de su comunicación mediante acceso, cesión, transmisión, transferencia, interconexión u otro mecanismo análogo. Esta clasificación cobra importancia en muchos aspectos, como por ejemplo, en la determinación del mercado secundario de datos personales, en la necesidad y contenido del consentimiento del titular de los datos, en el requerimiento de notificación del tratamiento, etc.

b) Según su naturaleza. Datos personales sensibles y no sensibles.

Esta sea una de las clasificaciones de mayor importancia, a partir de ella se distinguen dos grandes grupos o tipos de datos respecto de los cuales la gran mayoría de las legislaciones otorgan grados de protección de diversa intensidad, dada su distinta naturaleza. Los datos personales sensibles, son la excepción, operando la definición de los no sensibles por exclusión.

Existe un acuerdo bastante amplio, tanto en la legislación como en la doctrina y jurisprudencia, que este tipo de datos se refieren al origen racial y color de la piel; opiniones políticas; convicciones o actividades religiosas o filosóficas -o su ausencia-; adhesión a sindicatos; conducta sexual y salud que comprende información sobre el estado físico o mental, pasado, presente o futuro de la persona interesada y la información sobre el abuso de drogas o alcohol, etc.[107]. Como se puede observar de los ejemplos transcritos se trata de información personal, a partir de la cual es posible se puedan efectuar discriminaciones arbitrarias respecto de la persona a la cual se refieren. Por lo anterior, es que las legislaciones establecen requisitos más estrictos en cuanto a su tratamiento, operando como la gran regla general en esta materia, la prohibición de efectuarlo, salvo exista consentimiento previo y expreso del titular respectivo. Respecto de los datos no sensibles, que como ya señaláramos operan por exclusión, el grado de protección que le otorgan las legislaciones es por lo general menor que a los datos sensibles, estableciendo respecto de ellos mayores excepciones al consentimiento previo.

c) Según el tipo de registro del cual proceden. Datos públicos y no públicos.

La distinción se efectúa a partir de la disponibilidad del dato personal para quien quiera acceder a él. Así, la información personal que se encuentra disponible para cualquier interesado por encontrarse en registros o lugares de fácil acceso al público, como resultados de censos, bases de datos de registros oficiales, repertorios de jurisprudencia, archivos de prensa, directorio de teléfonos y otros de similar registro, constituyen datos públicos[108]. Por el contrario, datos no públicos son aquellos que presentan algún grado de restricción en su acceso, de manera que no cualquier persona puede acceder a ellos. La distinción cobra importancia en algunas legislaciones como la nuestra que recogen el concepto de fuente accesible al público, el cual permite efectuar tratamiento de ciertos datos que se encuentran en este tipo de registros, sin la autorización previa del titular de ellos, en las tres hipótesis que indica la ley[109].

[107] PUCCINELLI, Oscar. op.cit. pág. 54.
[108] GOZAINI, Osvaldo. op.cit. pág. 235.
[109] Este tema será tratado en profundidad en el capítulo II siguiente.

1.3.6. Los bancos o ficheros de datos personales

Los bancos o ficheros de datos personales se definen como el lugar en donde se encuentra un conjunto organizado o estructurado de datos de carácter personal cualquiera sea su forma de creación, almacenamiento, organización y acceso[110]. De su parte, el Diccionario de la Real Academia de la Lengua Española, define fichero como "Conjunto organizado de informaciones almacenadas en un soporte común" y banco de datos como "Acopio de datos referidos a una determinada materia, que puede ser utilizado por diversos usuarios". Las definiciones anteriores se ven reflejadas en mayor o menor medida en las conceptualizaciones que diversos cuerpos normativos sobre la materia efectúan de los bancos o ficheros de datos personales[111], las cuales permiten determinar sus elementos esenciales: en primer lugar, se debe tratar de un conjunto organizado de datos personales, es decir, que los datos personales que se encuentran almacenados en el banco de datos, deben presentar cierto grado de relación, disposición y orden a objeto de cumplir con un fin determinado (el entregar información personal); de esta manera, no será un banco de datos un simple registro de datos personales que no presenten una estructura, una organicicidad, una relación entre sus distintos elementos. En segundo lugar, y teniendo claro que se requiere de organización en la información personal que se contiene en los bancos de datos, la forma que adquiere esta organización es transparente para el legislador, ya que es indiferente las modalidades de su formación, creación, almacenamiento, acceso, etc. Por último, y en algunas legislaciones como la chilena y la argentina, el banco de datos puede ser tanto automatizado como no, lo que implica que queda dentro del ámbito de aplicación de la norma, tanto aquellos ficheros que son computacionales como los manuales; lo

[110] RUIZ, Antonio. Los datos de carácter personal: concepto, requisitos de circulación, procedimientos, normativa y formularios. 1999. Barcelona, Bosch. 208p. pág. 71.

[111] Así la Directiva Europea 95/46/CEE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos define fichero de datos personales como "todo conjunto estructurado de datos personales, accesible con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica". En nuestro país, la Ley 19.628 en su artículo 2 letra m) define al registro o banco de datos como "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". La ley argentina N° 25.326 de protección de los datos personales hace sinónimos los vocablos archivo, registro, base o banco de datos, señalando, que éstos designan, indistintamente, al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

anterior, en orden a que el ámbito de aplicación de las legislaciones protectoras de datos sea más amplio.

1.3.7. Las etapas del tratamiento

Por tratamiento de datos debemos entender una serie de operaciones y procedimientos técnicos efectuados ya sea a través de medios automatizados o manuales, que permiten efectuar respecto de los datos personales una serie de acciones, como por ejemplo, recogerlos o recolectarlos, grabarlos, almacenarlos, conservarlos, elaborarlos, modificarlos, eliminarlos, bloquearlos, cederlos, comunicarlos, transmitirlos, transferirlos, interconectarlos, etc. Respecto de este concepto, el cual ha sido construido fundamentalmente en base a la antigua ley de protección de datos personales española (la LORTAD) y a la Directiva Europea, cabe destacar que "se trata de una serie de operaciones y procedimientos para realizar una serie de actos en los que se utilizan los datos de carácter personal y que, cada uno de ellos, constituye por sí mismo, una forma de tratamiento de datos"[112]. Así por ejemplo, la sola operación de recogida de datos personales, ya implica que se está efectuando tratamiento de datos personales, en este sentido, Manuel Heredero[113] indica que "el hecho de que se incluyan dentro de la misma definición de tratamiento un conjunto de operaciones diversas que pueden reconducirse a operaciones aritméticas o lógicas, o ambas, no implica que el tratamiento constituya un todo indivisible, compuesto de todas esas operaciones; un tratamiento puede estar compuesto de una sola o de varias o de todas las operaciones enumeradas".

Del mismo concepto de tratamiento de datos podemos reconocer que en él existen distintas etapas o momentos, respecto de los cuales los autores coinciden[114]: Las etapas que se reconocen son tres, a saber: a) la etapa de la toma, recolección o recogida de datos personales; b) la etapa del tratamiento de datos propiamente tal, en la cual los datos son tratados --generalmente de forma automatizada-, permitiendo efectuar cruces y relaciones entre los datos; y, c) la etapa de cesión o comunicación de los datos a terceros ajenos a aquél que efectúa el tratamiento en

[112] RUIZ, Antonio. op.cit. pág. 70.
[113] HEREDERO, Manuel. La Directiva Comunitaria de Protección de los Datos de Carácter Personal. 1997. Madrid, Editorial Aranzadi. 372 p. pág. 86.
[114] DAVARA, Miguel Angel. Manual de Derecho Informático. 1997. Madrid, Editorial Aranzadi. 396 p. pág. 66. BAUTISTA Rafael. Protección Jurídica de datos personales automatizados. 1993. Madrid, Editorial Colex. 272p. pág. 96.

cuestión[115]. La importancia de la distinción está dada por la forma diferenciada en que las leyes de protección de datos y sus principios informadores regulan las distintas etapas del procedimiento, estableciendo el cumplimiento de deberes, requisitos y principios de diversa naturaleza, como señala Miguel Angel Davara[116] "estos tres momentos tendrán incidencia al fijar los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que les permitan ejercer sus derechos". En este mismo sentido se pronuncia Osvaldo Gozaíni[117] cuando indica que "A partir de la formación de un archivo, los datos personales que se compilan atraviesan por etapas y procedimientos distintos que van generando cuestiones jurídicas que deben analizarse puntualmente".

Lo usual es que estas etapas estén todas presentes en el tratamiento de un específico dato personal, pero como ya lo expresáramos, basta que se realice una sola operación dentro de cualquiera de las etapas para que estemos en presencia de tratamiento de datos personales.

1.3.8. Las leyes de protección de datos personales. Análisis Comparado.

1.3.8.1. Antecedentes previos

Las denominadas "Leyes de Protección de Datos", y en general, las normativas que regulan el tratamiento de datos personales, tanto a nivel nacional como supranacional, comparten determinada estructura y contenidos, es así como éstas señalan, en primer lugar, su ámbito de aplicación y ciertos principios generales en materia de tratamiento de datos personales, asimismo, establecen cuáles son los derechos y obligaciones de las partes involucradas en este tratamiento (titulares de los datos y titulares de los bancos de datos), las vías para hacer efectivo el ejercicio de los derechos de los titulares de los datos y el cumplimiento de las obligaciones por parte de los responsables o titulares de los bancos de datos, ya sea en sede administrativa o judicial, además, un porcentaje importante de ellas, crea una entidad administrativa (autoridad de control) cuya función es velar y fiscalizar la observancia de la normativa, finalmente terminan

[115] Si bien es cierto que la doctrina está conteste en estas tres etapas, cabe destacar que la tercera no necesariamente estará en todos los casos de tratamiento de datos presente, ya que puede darse el caso, aun cuando poco usual, que el tratamiento de datos se efectúe sin la existencia de una cesión o transferencia posterior de los datos que son tratados.
[116] DAVARA, Miguel Angel. 1997. Ib.
[117] GOZAINI, Osvaldo. op.cit. pág. 255.

estableciendo las sanciones y el régimen de responsabilidad a los que se verán sujetos los infractores a sus preceptos. A este respecto Renato Jijena, indica que las leyes sobre protección de datos se estructuran en cuatro partes, a saber: dogmática, orgánica, procedimental y represiva o sancionatoria[118]. Esta similitud de contenidos, que permite efectuar clasificaciones de este tipo deriva del hecho, que la gran mayoría de estas normativas se inspiran en el modelo europeo de protección de datos.

Es posible intentar una clasificación de las leyes de protección de datos en leyes omnicomprensivas (como la chilena) y leyes sectoriales. Las primeras aplican al tratamiento de datos que efectúe cualquier entidad, tanto pública como privada y respecto a cualquier tipo de dato, es el modelo que han preferido mayormente los países que han legislado en la materia y la Unión Europea. Las segundas, son leyes que regulan específicos tratamientos de datos, como por ejemplo los financieros, este es el modelo que ha adoptado Estados Unidos; la principal crítica a este modelo es que se debe estar continuamente legislando a medida que la tecnología avanza y aparecen nuevos tratamientos de datos personales que pueden implicar una amenaza a la privacidad, como por ejemplo ocurre en la actualidad en Estados Unidos con los datos genéticos[119].

Veremos a continuación, brevemente, el desarrollo del estado de las leyes de protección de datos en derecho comparado.

---

[118] JIJENA, Renato. La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos. 2001. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5. pp. 85-111.

[119] En todo caso, no sólo las leyes constituyen modelos de protección a la privacidad informacional. Así lo indican Albert Marcella y Carol Stucki, al señalar la autorregulación y las tecnologías como modelos de protección. Respecto de la primera indican que la protección de los datos puede ser conseguida, a lo menos en teoría, a través de varias formas de autorregulación en las cuales las empresas e industrias establecen códigos de conducta. Sin embargo, reconocen que en varios países y en especial en Estados Unidos, este modelo no ha cumplido ya que los códigos no son regularmente acatados. Este modelo es aplicado aun cuando no en forma exclusiva, en Estados Unidos, Japón y Singapur. Respecto de la tecnología, la cual resulta interesante como forma de autoprotección, estos autores indican que con el desarrollo reciente de tecnología comercialmente disponible la protección de la privacidad se ha puesto en manos de los propios individuos. Se trata de tecnologías de encriptación, correo electrónico anónimo, dinero digital, tarjetas inteligentes, entre otros. MARCELLA, Albert y STUCKI, Carol. op. cit. pág. 72.

1.3.8.2. Europa

En los años ´70 surgieron las primeras leyes protectoras de datos, ante la utilización cada vez más frecuente de procedimientos automatizados de tratamiento de la información en computadoras o máquinas, procedimientos que a los ojos de los legisladores aparecían como potencialmente peligrosos para los intereses y derechos de los ciudadanos, especialmente en relación a su intimidad o privacidad. Es en Europa y específicamente en la entonces República Federal de Alemania, en donde se dicta la primera ley de esta naturaleza en 1970, la Datenschutz, que en todo caso, tiene un alcance restringido, ya que sólo se aplica a los órganos públicos, es decir, organismos que efectúan tratamiento de datos de los ciudadanos, a esta ley, le sigue la Data Leg, de Suecia, dictada en 1973, que establecía un sistema de registro previo como requisito de existencia de los bancos de datos personales[120].

A estas primeras legislaciones le siguieron, las provenientes de otros países europeos, como Dinamarca, Noruega, Francia y Austria, entre los años 1978 y 1979[121].

Sin embargo, no es sino hasta 1981, con la dictación del Convenio de Estrasburgo[122], que se establecen determinados principios y normas comunes para los países que forman parte del entonces Consejo de Europa, cuyo objeto es, según lo señala su artículo 1, "garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos personales de carácter personal correspondientes a dicha persona".

[120] CERDA, Alberto. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. 2003. Tesis para optar al grado de magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho. 260p. pág.28.
[121] GONZALEZ, Francisco. Modelos comparados de protección de la información digital y la ley chilena de datos de carácter personal. 2001. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5. pp. 153-178.
[122] CONSEJO DE EUROPA. 1981. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Agosto 1981.

El Convenio de Estrasburgo fue el antecedente de la dictación en el año 1995 de la Directiva 95/46/CE[123], a través de la cual la Unión Europea decide armonizar las legislaciones de los diversos países a través de una Directiva sobre la materia[124] cuyo considerando segundo indica su finalidad esencial: "Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos".

Podemos observar un cambio respecto de la declaración de principios que a este respecto efectuaba el Convenio de Estrasburgo, ya que la Directiva reconoce que los sistemas de tratamiento de la información deben contribuir al progreso económico y social. Los aspectos regulados por la Directiva son los siguientes:

- Garantiza el respeto de los derechos de los titulares de datos, en lo que respecta al tratamiento de los datos personales y la libre circulación de datos personales entre los Estados miembros.
- Establece una serie de principios relacionados con la calidad de los datos, como, el de licitud, buena fe, consentimiento, finalidad, información, seguridad, etc.[125]
- Regula como una categoría especial de datos a los sensibles, estableciendo mayores niveles de protección.
- Indica los derechos de los titulares de datos, oposición, información o acceso, rectificación, supresión o bloqueo de los datos y las excepciones a su ejercicio.
- Establece los recursos judiciales, responsabilidades y sanciones.
- Regula la transferencia de datos personales a países terceros.
- Establece la necesidad de los códigos de conducta.
- Crea la autoridad de control, autoridad pública que se encarga de vigilar la aplicación de las disposiciones relativas al tratamiento de datos personales.

[123] UNION EUROPEA. 1995. Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Octubre 1995.
[124] PALAZZI, Pablo. La transmisión internacional de datos personales y la protección a la privacidad. 2002. Buenos Aires, Ad-hoc. 416.p

Las materias referidas, son las que luego, fueron adoptadas por los países miembros de la Unión Europea en sus legislaciones internas[126] y con mayor o menor fuerza en Latinoamérica y otros países del mundo.

Con posterioridad a esta Directiva, la Unión Europea ha dictado otras relacionadas con el tratamiento de datos personales en el ámbito de las telecomunicaciones o comunicaciones electrónicas, así en el año 1997, dicta la Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[127], que fuera posteriormente derogada por la Directiva sobre la privacidad y las comunicaciones electrónicas[128], que tiene un ámbito de aplicación restringido, ya que sólo se aplica a los servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad, de manera que el tratamiento de datos que se efectúa en redes cerradas de comunicación queda fuera de la aplicación de esta Directiva. La Directiva en comento regula aspectos relacionados con la seguridad de las redes, confidencialidad de las comunicaciones, datos de tráfico, comunicaciones no solicitadas, entre otras.

En la actualidad, debido a estas Directivas cuya armonización a las legislaciones internas de los países miembros de la Unión Europea es obligatoria, se puede afirmar que en Europa la normativa sobre protección de datos personales es uniforme, presentándose sólo leves diferencias sobre la base que establecen las Directivas revisadas.

1.3.8.3. Estados Unidos

La regulación normativa del tratamiento de datos en Estados Unidos, presenta diferencias importantes con la existente en la Unión Europea. En primer lugar, las leyes dictadas

---

[125] El necesario desarrollo de estos principios se efectuará cuando se revise los principios adoptados en estas materias en el acápite siguiente.
[126] Actualmente todos los países miembros de la Unión Europea cuentan con legislaciones omnicomprensivas de protección de tratamiento de datos personales.
[127] UNION EUROPEA. 1997. Directiva 97/66/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Diciembre 1997.
[128] UNION EUROPEA. 2002 Directiva. 2002/58/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Julio 2002.

sobre la materia presentan un carácter sectorial, no existiendo, consecuentemente una regulación omnicomprensiva del tratamiento de datos; la autorregulación ocupa un lugar esencial, de manera que una autoridad de control como la europea no se conoce en el sistema norteamericano; consecuentemente el nivel de protección a los titulares de datos en Estados Unidos, se presenta disminuido en relación al existente en la Unión Europea y otros países que han adoptado el modelo europeo. No obstante lo anterior, "la *Federal Trade Comisión* tiene poderes para exigir el cumplimiento de las leyes que protegen la privacidad de los niños en Internet, la información de crédito de los consumidores, como asimismo propende prácticas de comercio justo, pero no tiene autoridad general para exigir el cumplimiento de los derechos de privacidad"[129].

Francisco González[130] señala que la protección de la intimidad de la información digital en Estados Unidos se efectúa a través de tres sedes, a saber: leyes especiales sobre privacidad, las que analizaremos más adelante, principios constitucionales y acciones basadas en el *common law*.

Respecto a los principios constitucionales, este autor, indica que no obstante, la Constitución de los Estados Unidos no menciona la palabra "privacidad", existen amplios debates constitucionales en su nombre, no existiendo en materia de intimidad de la información pronunciamientos claros de la Corte Suprema.

En relación a las acciones basadas en el *common law*, señala González, citando a Gellman[131] el problema es que la protección que pueden otorgar las acciones nacidas de los ilícitos por violación de privacidad del *common law* es por completo insuficiente, ya que lo ilícitos clásicos de privacidad probablemente no podrán inducir o forzar al titular de la base de datos a publicar descripciones de los sistemas de registro, a limitar sus prácticas de recopilación de información, a cumplir con estándares de calidad de la información, a permitir acceso y corrección individual, o a restringir usos internos de la información.

[129] MARCELLA, Albert y STUCKI, Carol. op. cit. pág. 130.
[130] GONZALEZ, Francisco. op. cit. p. 165
[131] GELLMAN, Robert. Does privacy law work? EN: Philip E. Agre and Marc Roenberg editors, Technology and Privacy: The new landscape. (Massachusetts Institute of Technology, 1997), p.203.

Por último, en relación a la legislación de protección de datos en Estados Unidos, como ya hemos indicado su característica esencial es ser de carácter sectorial, y por lo mismo, muy profusas en cantidad. Ellas se han ido dictando a medida que las tecnologías han ido permitiendo el tratamiento automatizado de datos, en los distintos sectores o ámbitos de la sociedad. Así, en el año 1970, coincidente en la época, a lo menos, con la aparición de este tipo de normativa en Europa, se dicta la primera ley sobre tratamiento de datos personales, la *Fair Credit Reporting Act,* de 26 de octubre**,** que se refiere a la recogida, conservación y transmisión a terceros de informes sobre la solvencia personal, profesional o económica de las personas, estableciendo ciertos derechos a los afectados[132]; en 1974 se dicta la *Privacy Act*[133], la que, al igual que la primera ley alemana de protección de datos, sólo se aplica al Estado y sus organismos. Luego, dentro del ámbito de los datos patrimoniales se dicta la *Right to Financial Privacy*[134], de 1978, referida a la tutela de los datos financieros, en el mismo año la *Electronic Fund Transfer Act*[135] establece la obligación de las instituciones financieras que efectúen transferencias electrónicas u otros servicios bancarios por ese procedimiento, de informar a sus clientes del acceso de terceras personas a sus bancos de datos. Un tiempo después, en 1986, se dicta la *Electronic Communication Privacy Act*[136]**,** que prohíbe la interceptación de mensajes mandados por medios electrónicos, estableciendo sanciones civiles y penales por infringir la normativa. En 1988, se dicta una ley que trata específicamente al tratamiento de datos personales dentro de las agencias federales y que modifica la *Privacy Act* de 1974, es la *Computer Matching and Privacy Protection Act*[137]**,** en el mismo año se dicta la *Video Privacy Protection Act*[138] la cual fue dictada en reacción a la divulgación en un periódico de los registros de videos arrendados por un ministro de la Corte Suprema, Robert Bork, esta ley prohíbe la divulgación de datos personales sobre los arriendos de videos. Además, existen numerosas leyes estatales que regulan, también en forma sectorial, la protección de datos en distintos ámbitos, así podemos encontrar leyes que

[132] Esta ley ha sido modificada en varias ocasiones, la última fue en el año 2003, a través de la "Fair and Accurate Credit Transactions Act of 2003'' To amend the Fair Credit Reporting Act, to revent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes. Public Law 108-159. 108th Congress.
[133] 5 USC Sec. 552a. Esta ley también ha sido enmendada en varias ocasiones, las últimas a través de la ley Computer Matching and Privacy Protection Act of 1988.
[134] 12 U.S.C. 3401 et seq. Modificada por última vez en el año 2001, a través de USA Patriot Act of 2001: Section 358 to permit the disclosure of financial information to any intelligence or counterintelligence agency in any investigation related to international terrorism.
[135] (15 U.S.C. Sec. 1601 et seq.)
[136] (18 U.S.C. § 2703(d))
[137] (5 U.S.C. 552a(o) et seq.)
[138] (18 U.S.C. § 2710)

norman el tratamiento de datos personales sobre arrestos, información bancaria, de seguros, de empleo, de impuestos, datos médicos, estudios, correos electrónicos, abonados a televisión por cable, número de seguridad social, etc.[139] Como se puede observar, las leyes de privacidad en materia de protección de datos en Estados Unidos son de carácter sectorial, tanto a nivel federal como estatal y abarcan datos de carácter personal de la más variada índole.

Dado que el nivel de protección en Estados Unidos a los datos personales no era adecuado para la Unión Europea, ésta le exigió para permitir la transferencia internacional de datos personales a ese país, que cumpliera con ciertos requisitos mínimos, los que luego, de arduas negociaciones se plasmaron en un documento conocido como "Principios de Puerto Seguro"[140], estos principios son los siguientes[141]:

1) Notificación. Las entidades[142] informarán a los particulares:

a) de los fines con los cuales se recogen y utilizan información sobre ellos.

b) la forma de contactar con ellos para cualquier pregunta o queja.

c) los tipos de terceros a los cuales se revelará la información.

d) las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación.

2) Opción. Las entidades ofrecerán a los particulares la posibilidad de decidir (exclusión) si su información personal:

a) puede divulgarse a un tercero[143], o

---

[139] Para una completa enumeración de este tipo de legislación, ver. ELECTRONIC PRIVACY INFORMATION CENTER. [EN LÍNEA] <http://www.epic.org/privacy/consumer/states.html#wash> [consulta: 25 marzo 2005].

[140] Publicados por la Federal Trade Commission el 21 de Julio de 2000. Los principios de Puerto Seguro, son fundamentalmente los mismos que se adoptaron por la OCDE en 1980 en un documento denominado "The guidelines on the protection of privacy and transborder flows of personal data" y por la Asamblea General de las Naciones Unidas en resolución 45/95 de 14 de diciembre de 1990, denominados "Principios rectores para la reglamentación de los ficheros computarizados de datos personales".

[141] Se efectúa en esta parte, un resumen de los principios de Puerto Seguro.

[142] La adhesión a los principios de Puerto Seguro es absolutamente voluntaria. En todo caso, las entidades que decidan adherirse a los principios deben aplicarlos para obtener y conservar las ventajas de Puerto Seguro y declararlo públicamente.

[143] La notificación o la opción no son necesarias cuando la información se revela a un tercero que ejecute un cometido, como agente, en nombre y bajo las instrucciones de la entidad. No obstante, en este caso, sí se aplica el principio de transferencia ulterior.

b) puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida, o

c) no haya sido autorizado posteriormente por el particular.

Se deben proporcionar a los particulares mecanismos claros y transparentes, fácilmente disponibles y asequibles para ejercer su derecho de opción.

Si se trata de datos sensibles sobre la opción de participar debe ser afirmativa o explícita (aceptación) si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de información o de una manera distinta a la autorizada con posterioridad por éste al optar por la aceptación. En cualquier caso, una entidad debe tratar como delicada toda información recibida de un tercero cuando dicho tercero la identificación y la trata como información delicada.

3) Transferencia ulterior. Para revelar información a terceros deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actúe como agente, podrá hacerlo si previamente se asegura de que éste:

a) suscribe los principios

b) si es objeto de una resolución sobre su "adecuación" con arreglo a la Directiva y otra disposición o,

c) si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios.

Si la entidad cumple estos requisitos, no será responsable (a menos que la propia entidad acuerde lo contrario) del tratamiento realizado por el tercero a quién haya transferido este tipo de información y que cumpliere las limitaciones o estipulaciones establecidas, a menos que la entidad sepa, o debiera saber, que el tercero realizaría dicho tratamiento y no haya adoptado medidas razonables para impedir o detener el tratamiento.

4) Seguridad. Las entidades que creen, mantengan, utilicen o difundan información personal tomarán prevenciones razonables para evitar su pérdida, mal uso, consulta no autorizada, divulgación, modificación y destrucción.

5) Integridad de los datos. La información de carácter personal, de acuerdo con los principios, debe ser pertinente para los fines con que se utiliza. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular. En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.

6) Acceso. Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar, suprimir dicha información si resultase inexacta excepto en los casos siguientes: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleva para la vida privada de la persona; o cuando puedan vulnerar los derechos de otras personas.

7) Aplicación. Se incluirán mecanismos para garantizar la conformidad con los principios. Tales mecanismos deben incluir:

a) una vía de recurso independiente, asequible e inmediatamente disponible para investigar y resolver con arreglo a los principios las denuncias y litigios de los particulares y otorgar daños y perjuicios donde determinar la legislación aplicable a las iniciativas del sector privado.

b) procedimientos de seguimiento para comprobar que los certificados y declaraciones de las empresas sobre sus prácticas en materia de vida privada se ajustan a la verdad y que dichas prácticas se aplican en consecuencia.

c) obligación de subsanar los problemas derivados del cumplimiento de los principios para las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán suficientemente rigurosas para garantizar su cumplimiento.

No obstante haber adoptado estos principios, su aplicación práctica ha sido más bien restringida, debido a como indica Alberto Cerda la pluralidad de disposiciones legales aplicables, el mosaico de instituciones comparecientes como autoridades de aplicación, las restringidas facultades conferidas a éstas para velar por el cumplimiento, así como los márgenes

de autoregulación, la fiabilidad de la autocertificación y el escaso número de entidades y organismos que han hecho propios los principios de *Safe Harbor*.[144]

1.3.8.4. Latinoamérica

La característica esencial de las legislaciones protectoras de datos Latinoamérica, ya sea omnicomprensivas o sectoriales, es encontrarse inspiradas en el modelo europeo de protección, pero sin uno de sus elementos esenciales: el órgano de control[145]. El otro elemento de importancia a considerar, es que la mayoría de los países latinoamericanos no cuentan con una legislación regulatoria omnicomprensiva de la actividad de tratamiento de datos personales[146], sino que sectorial, es decir, sólo algunos ámbitos del tratamiento de datos personales encuentran marco normativo, generalmente asociado a datos de carácter patrimonial (financieros, económicos, comerciales) o relacionados con normas de protección a los consumidores. Es interesante, además, observar que al igual que algunos países europeos, ciertos estados en Latinoamérica efectúan un reconocimiento constitucional, con mayor o menor amplitud, a la protección de datos a través del establecimiento de la autodeterminación informativa, entendida como la posibilidad de control de la propia información que poseen terceros[147].

1.3.9. Principios.

Existen en el ámbito de la protección de datos personales, ciertos principios que constituyen parámetros mínimos que deben guiar a las distintas legislaciones protectoras de datos. Tales principios han sido establecidos por organismos internacionales, como la Organización de Cooperación y Desarrollo Económicos a través de su "Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de

---

[144] CERDA, Alberto. op.cit. pág.52. En este mismo sentido, ver: MARCELLA, Albert y STUCKI, Carol. op cit. pág. 75.

[145] Sólo la Ley 25.326 argentina de Protección de Datos contempla la existencia de un órgano de control. Pablo Palazzi da cuenta de esta realidad señalando que la expansión del modelo europeo también está teniendo lugar en Latinoamérica. Aunque muchos países aún no cuentan con una ley de protección de datos, en general, varios han incluido en sus textos constitucionales cláusulas relativas a la privacidad o hábeas data en la última década; también se han aprobado leyes de privacidad, y existen varios proyectos de leyes de protección de datos personales basados en las ideas europeas. PALAZZI, P. op.cit. pág. 43

[146] Actualmente sólo la tienen Argentina, Chile y Paraguay.

datos personales", adoptada por el Consejo de ministros de esta organización el 23 de septiembre de 1980, el Consejo de Europa con la "Recomendación de la Comisión 81/670/CEE relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" de 29 de julio de 1981, la Organización de las Naciones Unidas por medio de los "Principios rectores para la reglamentación de los ficheros computarizados de datos personales", adoptado por la Asamblea General de las Naciones Unidas en su resolución 45/95 de 14 de diciembre de 1990. A efectos de nuestro análisis y dada la importancia de estos principios, los trataremos a continuación[148]:

1.3.9.1. Principio de la licitud y lealtad

Conforme este principio los datos personales no se deberían recoger ni elaborar con procedimientos desleales o ilícitos. La licitud en el tratamiento, implica por supuesto, que todas las operaciones que se efectúen en relación con los datos personales, cumplan con la normativa en la materia, pero también que tales operaciones sean leales, como señala Osvaldo Gozaíni, "la licitud en la recolección de datos supone que las acciones emprendidas para la obtención de informaciones personales han dado cumplimiento a una pauta general de buena fe y lealtad hacia las personas interesadas"[149]. Es así, que cualquier acción que implique ocultación, engaño, apariencia, sigilo o cualquier otra maniobra elusiva de la verdad, constituirán un acto desleal en el tratamiento de datos personales. Para David Bainbridge[150], "si los datos personales han sido obtenidos del titular de los datos o de otra persona mediante engaño, entonces el procesamiento será desleal…Pero la deslealtad va más allá de lo anterior. Un procesamiento leal también requiere que el titular de los datos sea informado de cualquier uso no obvio por el responsable del tratamiento al momento en que el dato es recolectado".

---

[147] Así ocurre en Argentina, Brasil, Colombia, Ecuador, Guatemala, Nicaragua, Paraguay, Perú, y Venezuela. Para un completo análisis de la legislación comparada en materia de protección de datos en Latinoamérica ver: JAÑA Washington. op.cit.

[148] Nos guiaremos a estos efectos fundamentalmente por los principios de la Naciones Unidas, por ser directrices generales y flexibles, ya que su propósito es que sean incorporadas a las legislaciones internas de los países.

[149] GOZAINI, Osvaldo. op.cit. pág. 195.

[150] BAINBRIDGE, David. Data Protection Law. 2ª ed. 2005. Great Britain, xpl publishing. 328p. pág. 62.

1.3.9.2. Principio de la calidad de los datos.

Este principio exige que los datos personales respecto de los cuales se efectúa tratamiento sean de calidad, esto es, que sean exactos y pertinentes, de manera que se establece la obligación para aquél que trata datos personales de verificar la exactitud[151] y pertinencia de los datos registrados, como asimismo, cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando. Este principio está íntimamente vinculado con el principio de finalidad que se tratará más adelante, Ana Herrán indica a este respecto que el principio de calidad de los datos se debe contemplar desde una doble perspectiva: la calidad del dato personal y la finalidad del tratamiento, de manera que los datos alcanzan determinada calidad y es lícito su tratamiento porque son puestos en relación con los fines legítimos que inspiran el tratamiento, y el dato será adecuado o pertinente cuando se encuentre directamente relacionado con la finalidad concreta, cuando sea necesario para el cumplimento de la misma, pero por otro lado, también será pertinente o adecuado cuando responda a la veracidad y exactitud e integridad de la información relativa a la persona[152].

1.3.9.3. Principio del consentimiento del titular de los datos.

Este principio establece que la regla general es que el titular de los datos deba prestar su consentimiento para que se pueda legítimamente efectuar tratamiento de su información personal, las excepciones a este principio deben ser establecidas por una norma legal[153]. La autorización o consentimiento consiste en un acto, por regla general, expreso del titular de los datos por el cual está de acuerdo en que su información sea incorporada a un banco o registro de datos personales. Antes de prestar el consentimiento, debe ser informado, a lo menos de la

[151] La exactitud como parte del principio de calidad de los datos genera la obligación de tomar todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los cuales fueron recogidos o para los cuales fueron tratados posteriormente, sean suprimidos o rectificados. Palazzi. Pablo. 2002. La Transmisión internacional de datos personales y la protección de la privacidad. Buenos Aires, Ad-Hoc. 409p. pág. 33.

[152] HERRÁN, Ana. 2002. El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales. Madrid, Dykinson. 388 p. pág. 211.

[153] La importancia y cantidad de excepciones legales a la regla general del consentimiento del titular de los datos que se contienen en las distintas legislaciones, es un tema central que debe de

finalidad del tratamiento y el destino que tendrán sus datos. La exigencia de este consentimiento es la base sobre la cual se estructura el derecho a la autodeterminación informativa, el cual busca que el tratamiento de datos se efectúe a partir de una decisión libre y voluntaria de las personas[154].

1.3.9.4. Principio de la seguridad de los datos.

Este principio exige que se adopten medidas apropiadas para proteger los bancos de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático. Como señala Osvaldo Gozaíni[155], este principio tiene dos facetas importantes: una atiende a la protección de los datos en particular; la otra al cuidado especial que se ha de tener con las personas que tratan la información y custodian la seguridad general del archivo. Podríamos establecer una distinción clara en base a lo señalado, se precisa un cierto grado de seguridad técnica que impida que la información se corrompa, destruya, o inutilice por casos fortuitos o "riesgos naturales", asimismo, se necesita seguridad lógica que impida que terceros no autorizados accedan a la información personal, que les permita por ejemplo, efectuar usos, modificaciones o divulgaciones indebidas de la misma. En fin, se requiere un comportamiento activo del responsable del banco de datos, es decir, que desarrolle las garantías y medidas necesarias para la seguridad del tratamiento y de los datos objeto del mismo[156].

1.3.9.5. Principio de la confidencialidad de los datos.

La Directiva Europea 95/46 en su artículo 16 establece este principio en los siguientes términos: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento de datos personales, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o en virtud de un imperativo legal. Cabe comentar respecto a este precepto que no establece la confidencialidad o

considerarse cuando se efectúe un análisis *in extenso* de este principio- cosa que escapa al objeto de esta tesis-.

[154] GOZAINI, Osvaldo. op.cit. pág. 265.

[155] GOZAINI, Osvaldo. op.cit. pág. 204.

secreto del tratamiento como una obligación de secreto profesional, sino como un deber de sujetarse en su actuación a las instrucciones o directrices del responsable del tratamiento, en cuanto los datos personales objeto del mismo[157]. Por último, a este respecto cabe distinguir entre conceptos que podrían llevar a confusión: privacidad, confidencialidad o secreto y seguridad referidos a los datos sometidos a tratamiento. La privacidad hace referencia a que los datos son de una persona y que ésta tiene derecho a controlarlos y saber cómo se van a utilizar; la confidencialidad se refiere al mayor o menor secreto en que se van a guardar y tratar esos datos; y, la seguridad hace referencia a las medidas de protección a tomar para la mejor defensa de la privacidad y grado de confidencialidad[158].

1.3.9.6. Principio de acceso

El principio de acceso dice relación con los derechos mínimos que se le deben asegurar a las personas en tanto titulares de su información, así se indica que toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios. Además se le deben explicar al titular de los datos las razones por la cuales las peticiones antes indicadas han sido denegadas, así como poder cuestionar tal denegación, para lo cual debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control. También tendrá derecho a expresar dudas sobre los datos relativos a su persona, y si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan. En caso de rectificación, el costo debería sufragarlo el responsable del banco de datos. Como podemos observar, este principio otorga derecho de acceso a los titulares de datos, respecto de la información que le concierne, para cerciorarse, en particular, de su exactitud y de la licitud del tratamiento, o dicho en palabras de Ana Herrán, "el derecho de acceso garantiza a la persona poder conocer la licitud de su tratamiento pero aún más también la licitud o calidad de los datos objeto del tratamiento"[159].

---

[156] HERRÁN, Ana. op.cit. pág. 239.
[157] HERRÁN, Ana. op.cit. pág. 164.
[158] DAVARA, Miguel Angel. 1998. La protección de datos en Europa. Principios, derechos y procedimiento. Madrid, Grupo Asnef Equifax. 204 p. pág. 24.

1.3.9.7. Principio de la finalidad

Junto con el principio del consentimiento, el de la finalidad es uno de los más importantes informadores del tratamiento de datos personales, ya que de alguna u otra manera se encuentra presente en las demás directrices, y porque, además, es de aquellos principios que deben respetarse en las distintas etapas del tratamiento. Conforme a él, la finalidad de un banco de datos y su utilización en función de esta finalidad deberían especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse que: a) Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida; b) Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; c) El período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado. Es decir, el objetivo que persigue el tratamiento de datos personales debe ser informado al momento de la recogida de estos datos, finalidad que debe perdurar durante todas las etapas posteriores del tratamiento, salvo que exista consentimiento del titular de los datos. Por último, una vez que se ha alcanzado a plenitud la finalidad del tratamiento, los datos personales de que se trate debieran ser eliminados.

---

[159] HERRÁN, Ana. op.cit. pág. 153.

CAPITULO SEGUNDO

ANALISIS DE LA NORMATIVA NACIONAL EN MATERIA DE PROTECCION DE DATOS PERSONALES, EN ESPECIAL DE LA LEY 19.628

2.1.- Marco regulatorio de la protección de datos personales en Chile.

La protección de datos personales en nuestro país encuentra fundamentos constitucionales y legales, lo que lleva a efectuar el análisis del marco regulatorio nacional en estas materias, distinguiendo entre la protección constitucional y la legal.

2.1.1. Protección constitucional.

Cabe indicar, en primer lugar, que a diferencia de varios ordenamientos jurídicos extranjeros[160], nuestro ordenamiento no reconoce constitucionalmente el derecho a la privacidad informacional. A este respecto, Oscar Puccinelli[161] ha señalado que existe discusión en la doctrina nacional respecto a si es necesario constitucionalizar este derecho, como partidario de la constitucionalización Héctor Nogueira indica que es imperioso reformar la Constitución para establecer el núcleo esencial del derecho a la autodeterminación informativa y regular los lineamientos procesales fundamentales, porque si bien este derecho puede deducirse actualmente de varios otros reconocidos en la Constitución, no sólo no estaría tutelado por la acción de protección, por no ubicarse en el artículo 19 de la Constitución, sino porque además resulta inconveniente que ésta abarque al hábeas data, porque, a diferencia de aquella, el ejercicio de ésta no debe quedar sujeto a caducidad, ni coincidir en cuanto a los efectos de la sentencia que rigen la protección. Por el contrario, Emilio Pfeffer indica que a su criterio no es necesario reformar la Constitución para incorporar el hábeas data, y que basta con una ley receptora de los principios elementales del tratamiento de datos personales, e instrumentalizar el instituto a través

[160] Así lo hacen con mayor o menor amplitud las constituciones latinoamericanas de Argentina (art. 43 inc. 3°), Brasil (art. 5 LXXII), Colombia (art. 15), Ecuador (art. 94 inc. 2°), Guatemala (art. 31), Nicaragua (art. 26 N° 4), Paraguay (art. 135) y Venezuela (art. 28).
[161] PUCCINELLI, Oscar. op. cit. pág. 338.

del recurso de protección. En la misma línea, para Mario Verdugo en esta temática no es cuestión de ser reglamentaristas en exceso, ni es imprescindible realizar regulación constitucional del hábeas data[162].

La protección de datos personales busca amparar diversos bienes jurídicos, no obstante ser el principal el derecho a la privacidad o intimidad. Este derecho se encuentra garantizado en nuestra Constitución Política de la República de 1980, en el artículo 19 N° 4, artículo ubicado en el Capítulo III sobre los Derechos y Deberes Constitucionales y que en su inciso primero proclama "El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia". Este artículo inexistente en la Constitución Política de 1925, protege diversos bienes jurídicos, de una parte: la vida privada y pública de las personas y de otra, la honra de la persona y de su familia. Se trataría de un derecho a poder estar solo si uno lo desea, a mantenerse apartado de la observación de los demás sin ser molestado, sin intromisiones en lo más personal de su vida[163]. Derecho que estaría relacionado con lo que en doctrina ya clásica se conoce como el "Derecho a ser dejado solo" o "*Right to be left alone*", es decir, con la concepción de *Privacy* como soledad o retiro. Sin embargo, nuestro constituyente parece ir más allá de este derecho, ya que junto con establecer y garantizar la privacidad de las personas, garantiza la honra de ellas y de sus familias. Concepto este último que efectivamente resulta diferenciable de la privacidad e intimidad. El honor, la honra, pueden ser apreciados desde dos puntos de vista, uno objetivo que está representado por la apreciación y estimación que hacen los demás de nuestras calidades morales y de nuestro valor social (la honra) y uno subjetivo que se corresponde al sentimiento de nuestra propia dignidad moral nacido de la conciencia de nuestras virtudes, de nuestros méritos (el honor) [164].

Seguidamente, el artículo 19 N° 5 asegura a todas las personas "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las

[162] De nuestra parte, creemos que no es necesario el establecimiento constitucional del derecho a la privacidad informacional, porque tanto la jurisprudencia, como asimismo, la doctrina ven la protección de este derecho, en diversas garantías constitucionales, especialmente, en la establecida en el artículo 19 N° 4 de la Constitución Política. De su parte, si bien la Ley 19.628 presenta importantes vacíos respecto a la entrega de un control y tutela efectiva del titular de los datos respecto a la información que le concierne, lo correcto desde un punto de vista de técnica legislativa es reformar la ley y no modificar la Constitución en el sentido que se comenta.
[163] Verdugo, Mario; Pfeffer, Emilio; Nogueira, Héctor. Derecho Constitucional. Tomo I. 1994 Ed. Jurídica de Chile. 365p. pág. 250.
[164] Verdugo, Mario; Pfeffer, Emilio; Nogueira, Héctor. op.cit. pág. 251.

comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley". La salvaguarda de la privacidad se vería seriamente dificultada si además y junto con su protección, no se estableciera la proscripción de la invasión ilegítima y/o ilegal al hogar y a las comunicaciones privadas. En relación a este último punto interesante resulta el contenido de una de las Actas de la Comisión de Estudio de la Nueva Constitución (Sesión N° 129), que deja constancia que el precepto comprende e incluye la defensa contra todas las formas modernas que permitan interceptar conversaciones a la distancia o captar imágenes, las que existen y se conocen en la actualidad o puedan en el futuro descubrirse.

Ambos artículos y los respectivos derechos que aseguran se encuentran entroncados en su base con el concepto de privacidad. Razón por la cual, es en base sobre todo al artículo 19 N°4 de la Constitución, que la gran mayoría de la jurisprudencia y de la doctrina nacional elabora la existencia de una protección de datos personales, cosa que ocurrió también en las discusiones legislativas que recayeron sobre el proyecto de ley sobre Protección a la Vida Privada que es justamente el que regula la materia en Chile.

El ámbito de protección constitucional se cierra con el numeral 26 del artículo 19 de la Constitución que impide que alguna ley complementaria, limitativa o reguladora de las garantías fundamentales las afecte en su esencia, les imponga condiciones, tributos o requisitos que impidan su libre ejercicio.

Además de los artículos anteriores necesariamente debemos recordar acá el artículo 5 inciso segundo de la Carta Fundamental chilena que obliga al Estado a respetar y promover los derechos esenciales de la persona humana, garantizados por la Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes[165].

[165] Declaración Universal de Derechos Humanos, Naciones Unidas, 1948. Art. 12. "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia o de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."
Pacto Internacional de Derechos Civiles y Políticos. Asamblea General de las Naciones Unidas, 1966. Art. 17. "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, su correspondencia, ni de ataques ilegales a su honra y reputación".
Convención Americana sobre Derechos Humanos, 1962. Art. 11. "Protección de la honra y de la dignidad."1. Toda persona tiene derecho al respeto de su honor y al reconocimiento de su dignidad. 2.

2.1.2. Protección legal.

Este tipo de protección podemos agruparla en dos grandes categorías:

I. Una primera categoría que está compuesta por normas de diversa naturaleza tanto en cuanto a su jerarquía, como en lo que respecta a sus ámbitos de aplicación, pero que tienen en común encontrarse relacionadas con la protección de datos personales.

De las anteriores normas sólo comentaremos aquellas que resultan más interesantes de señalar por su nivel de importancia y su aplicación.

a) Decreto Supremo Nº 950/1928 del Ministerio de Hacienda. Que regula el "Boletín de Informaciones Comerciales" de la Cámara Chilena de Comercio, señalando en forma taxativa quiénes deben entregar datos a la Cámara y la forma en que ésta debe poseer y publicar la información. Se trata acá de la regulación de datos patrimoniales. El artículo 3 transitorio de la Ley 19.628 ha indicado que las normas de este decreto supremo, seguirán aplicándose en todo lo que no sean contrarias a la referida Ley.

b) Código Sanitario. El artículo 127 de este cuerpo legal dispone que: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados" y sólo puede revelarse el contenido o darse copia de ellos "con el consentimiento expreso del paciente, otorgado por escrito". Luego señala que: "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 expendieron, ni datos que sirvan para identificarlos". También prescribe esta norma que la reserva 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[166]. La violación de lo prescrito por este artículo, será castigado en la forma y con las sanciones establecidas en el Libro Décimo de ese Código. Estamos acá en el ámbito de los datos sensibles, ya que se trata de datos relativos a la salud de las personas.

Nadie puede ser objeto de injerencias arbitrarias o abusiva en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."

c) Código Tributario: El artículo 30 inciso 4º de este código prescribe que: “las personas que, a cualquier título, reciban o procesen las declaraciones o giros quedan sujetas a obligación de reserva absoluta de todos aquellos antecedentes individuales de que conozcan en virtud del trabajo que realizan. La infracción a esta obligación será sancionada con reclusión menor en su grado medio y multa de 5 a 100 UTM”. Esta disposición establece el denominado secreto tributario o fiscal, el cual resguarda las informaciones relativas a la fiscalidad de los contribuyentes. Cabe llamar la atención en cuanto a que la norma no sólo es aplicable a los funcionarios del Servicio de Impuestos Internos, sino que también a los particulares que toman conocimiento de tales informaciones al recibir y procesar tales declaraciones tributarias, como lo son por ejemplo, los funcionarios bancarios que reciben tales documentos. Claramente, estamos en presencia de la regulación de algunas de las operaciones del tratamiento de datos tributarios.

d) Ley General de Bancos: El inciso primero del artículo 154 de la Ley General de Bancos, dispone que: “Los depósitos y captaciones de cualquiera naturaleza que reciban los bancos están sujetos a secreto bancario y no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente. El que infringiere la norma anterior será sancionado con la pena de reclusión menor en sus grados mínimo a medio”. Por lo tanto, la infracción a este deber de secreto es constitutiva de delito penal. Luego el inciso 2º de esa disposición señala que: “Las demás operaciones quedan sujetas a reserva y los bancos solamente podrán darlas a conocer a quien demuestre un interés legítimo y siempre que no sea previsible que el conocimiento de los antecedentes pueda ocasionar daño patrimonial al cliente”. Agrega el legislador en este mismo inciso que, no obstante lo anterior, y a objeto de evaluar la situación del banco, “éste podrá dar acceso al conocimiento detallado de estas operaciones y sus antecedentes a firmas especializadas, las que quedarán sometidas a la reserva establecida en la ley y, siempre que la Superintendencia las apruebe e inscriba en el registro que abrirá para estos efectos”. El inciso tercero del artículo 154 dispone por otra parte, que: “en todo caso, los bancos pueden dar a conocer las operaciones señaladas en los incisos anteriores, en términos globales, no personalizados ni parcializados, sólo para fines estadísticos o de información cuando exista un interés público o general comprometido, calificado por la Superintendencia”. Al respecto,

[166] Esta disposición fue introducida por el artículo 24 de la Ley 19.628.

debemos hacer presente que la Superintendencia de Bancos e Instituciones Financieras, en la Circular para Bancos Nº 2.544 de 8 de junio de 1990, ha señalado en relación a las informaciones que soliciten las instituciones del sector público a los bancos, que si bien aquellas instituciones se encuentran en la situación excepcional recién señalada cuando se requiera tal información para fines relacionados con la actividad que desarrollen, todas las peticiones de información que se hagan a los bancos e instituciones financieras deben ser canalizadas a través de la Superintendencia, a efecto de la calificación de la relación entre el antecedente solicitado y la función de la institución pública que pide la información[167]. Siguiendo con las excepciones al secreto bancario, el inciso 4º del artículo 154, dispone que: "la justicia ordinaria y la militar, en las causas que estuvieren conociendo, podrán ordenar la remisión de aquellos antecedentes relativos a operaciones específicas que tengan relación directa con el proceso, sobre los depósitos, captaciones u otras operaciones de cualquier naturaleza que hayan efectuado quienes tengan carácter de parte o inculpado o reo en esas causas u ordenar su examen, si fuere necesario". Finalmente, cabe anotar que mediante la Ley 19.806 de 31 de Mayo de 2002 se agregó un nuevo inciso final al artículo 154, en razón de la reforma procesal penal. Este nuevo inciso señala que: "los fiscales del Ministerio Público, previa autorización del juez de garantía, podrán asimismo examinar o pedir que se les remitan los antecedentes indicados en el inciso anterior, que se relacionen directamente con las investigaciones a su cargo". De manera tal que se regulan en el artículo en comento, la especie de datos patrimoniales denominados datos bancarios.

e) Ley 19.223 que tipifica figuras penales relativas a la informática: El artículo 2 de esta ley señala que **"**El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". En primer lugar, se hace necesario conceptualizar sistema de tratamiento de la información, coincidimos con Etcheberry[168] cuando señala que la ley al no distinguir se debe entender este concepto en un sentido amplio, y por ende comprende tanto el *hardware* como el *software* y todos los datos o información que en él se procesen. Como se puede colegir este tipo penal puede ser utilizado con

[167] La Circular anterior puede ser consultada SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS [en línea] <http://www.sbif.cl/NormasSBIF/Bancos/C2544B.pdf> [consulta: 9 de Mayo 2003]

el fin de tutelar la protección a los derechos de los titulares de datos, ya que castiga a aquél que se apodere, use o conozca indebidamente datos personales contenidos en un sistema de información, a través de un simple acceso, interferencia o interceptación. De su parte el artículo 4° indica que: “El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Por último, esta figura del artículo 4 también es una norma que puede brindar protección a los datos personales, en una determinada hipótesis, sólo que es más exigente que la revisada con antelación ya que acá se exige dolo directo en la comunicación a un tercero en específico o al público en general de los datos personales para que se configure el delito, circunstancia que será de difícil prueba.

II. La segunda categoría de normas está compuesta por aquellas que regulan en forma específica el tratamiento de datos personales en nuestro país, es decir, la Ley 19.628 sobre Protección a la Vida Privada, su reglamento promulgado por Decreto Supremo Nº 779/2000 del Ministerio de Justicia y la modificación efectuada por la Ley 19.812.

El objeto central de este capítulo es efectuar un análisis en profundidad de aquellas materias de esta segunda categoría normativa, las que resultan de especial importancia en el marco general de esta tesis, ya que constituyen la base legal del análisis que se efectuará en el capítulo siguiente[169]. De esta manera a continuación nos referiremos a temas centrales de la Ley 19.628, como por ejemplo, la determinación de los derechos asignados; su ámbito de aplicación; la autorización o consentimiento del titular de los datos; la transferencia o comunicación de datos a terceros; las categorías de datos reconocidas en la ley; los derechos subjetivos del titular de los datos; y, finalmente las reglas de responsabilidad, entre otros.

---

[168] Etcheberry, Alfredo. Derecho Penal. Parte Especial. Tomo III. 3ª ed. Actualizada. 1998. Ed. Jurídica de Chile. pág 271.

[169] El Capítulo III de esta tesis enfoca la regulación del mercado de datos personales a diferencia del presente capítulo que realiza el análisis jurídico tradicional.

2.2. La asignación de derechos.

La Ley 19.628 sobre Protección a la Vida Privada o de Protección de Datos Personales, publicada en el Diario Oficial el 28 de Agosto de 1999, tuvo su origen en una moción parlamentaria presentada por el Senador Cantuarias el 05 de enero de 1993, que buscaba "llenar un vacío en nuestro ordenamiento y cuyo propósito es buscar una adecuada protección al derecho de la privacidad de las personas, en el ámbito del Derecho Civil, ante eventuales intromisiones ilegítimas"[170].

La moción contemplaba disposiciones que determinaban la extensión de la vida privada (derecho a la propia imagen, intimidad personal y familiar, anonimato o reserva, vida tranquila sin hostigamientos ni perturbaciones; inviolabilidad del hogar y de toda otra forma de comunicaciones privadas), prohibía las intromisiones ilegítimas a ella, establecía mecanismos de protección frente a éstas, y otorgaba instrumentos de compensación ante eventuales daños morales y materiales que se produjeran por eventuales injerencias ilegítimas. Dentro del amplio objeto de esta moción, se contemplaba un Título II denominado "De la Protección de Datos", que luego de que la moción fuera conocida por la Cámara de Diputados quedó como el único ámbito de la privacidad regulado en el proyecto de ley.

Con la finalidad de determinar cuáles son las asignaciones de derechos efectuadas por la Ley 19.628, revisaremos a continuación la evolución que se produjo respecto a este punto en el proyecto de ley.

En la moción del senador Cantuarias, se indicaba en el artículo 6° que "El derecho a la vida privada es irrenunciable e imprescriptible, sin perjuicio de los casos de autorización previstos en la ley o de consentimiento del titular del derecho", luego a propósito del tratamiento de datos personales se reforzaba esta idea al establecer en el artículo 9° que "Sin perjuicio de los casos exceptuados en la ley, nadie podrá utilizar la informática para el procesamiento de datos de índole personal sin el consentimiento del titular". Es así, que en la moción, sólo se reconocía formalmente el derecho del titular de los datos a mantener el control de su información respecto

al tratamiento informático que de ella podían efectuar terceros, a través de la técnica de la autorización previa, se guardaba silencio respecto al derecho de terceros a tratar esa información.

Luego, en el primer informe de la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados, el proyecto pasó a denominarse "Proyecto de Ley sobre Protección de Datos de Carácter Personal"[171]. En él se vislumbran cambios fundamentales respecto a los derechos que se les otorgan a los actores involucrados en el tratamiento de datos, ya que el proyecto parte en su artículo 1° estableciendo que "Toda persona tiene derecho a recolectar, procesar, custodiar y transferir datos. Con el propósito de proteger a las personas por el uso que terceros pueden hacer de sus datos personales, la recolección, procesamiento y utilización de los mismos se sujetarán a las disposiciones de esta ley". Así el derecho o titularidad basal del proyecto se mueve desde el titular de los datos a aquellos que se dedican a efectuar el tratamiento de ellos, quienes en todo caso, deben estar autorizados para efectuar tal tratamiento por la ley en proyecto, por otras disposiciones legales o por la persona afectada.

En el segundo informe de la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados[172], vuelve a producirse un giro completo respecto a los derechos otorgados en el proyecto, ya que junto con establecer el derecho a efectuar tratamiento de datos personales, se le otorga expresamente al titular de los datos el derecho a la autodeterminación informativa o libertad informática, derecho que fuera reconocido por primera vez en la afamada sentencia del Tribunal Constitucional alemán sobre la Ley de Censo, pronunciado el 15 de diciembre de 1983, y que consiste en la potestad que tiene todo sujeto a controlar la información que de su persona tengan terceros.

El Senado al recibir el proyecto de ley con las modificaciones efectuadas por la Cámara de Diputados, las rechaza casi íntegramente, por lo que se decide formar una comisión mixta que dirima las discrepancias entre ambas cámaras. El Senado en el proyecto de ley que recomienda a la comisión mixta, elimina la mención al derecho a la autodeterminación informativa para los titulares de datos, dejando establecido el derecho a efectuar tratamiento de datos en el artículo

[170] Diario Sesiones del Senado. Sesión 20, tomo 2890, pág. 3079. 05 de enero de 1993.
[171] Esto debido a que el proyecto, como ya señaláramos, se restringió sólo a un ámbito de la privacidad, cual es, la protección de los datos personales. Diario Sesiones del Senado. Sesión 63, tomo 7482, pág. 7383. 17 de mayo de 1995.

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 buena fe, 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". La eliminación se justificó por el riesgo de consagrar en forma expresa un concepto doctrinario no suficientemente asentado y porque se entendió que el artículo primero entregaba un marco claro dentro del cual se puede efectuar el tratamiento de datos, esto es, respetando los derechos fundamentales del titular de los datos y la ley. Resulta interesante acotar aquí que el Senado recogió, al eliminar la mención a la autodeterminación informativa, la tesis expuesta por el Ministerio Secretaría General de la Presidencia, la que indica que "si bien la afirmación de este nuevo derecho (la autodeterminación informativa) ha sido seguida de cerca por los italianos y los españoles -y parte de nuestra doctrina, como los profesores de Derecho Constitucional señores Humberto Nogueira y Francisco Zúñiga-, no es pacífica en la propia Alemania. Parte de la doctrina señala el riesgo de incurrir en una consideración patrimonialista del nuevo derecho en caso de seguirse esta corriente, en razón a que induce a pensar que las personas ostentan un derecho de propiedad sobre sus datos"[173].

Finalmente, la comisión mixta acogió la propuesta del Senado y se aprobó más o menos en dichos términos el artículo 1°, que luego sería el artículo 1 de la Ley 19.628[174].

De lo dicho, se puede concluir que existió durante toda la tramitación del proyecto de ley cierta confusión en el legislador respecto a los derechos a otorgar a los sujetos regulados en la ley, y que al momento de decidir a quién otorgarlos y en qué forma, se optó por asignar en el

[172] Diario Sesiones del Senado. Sesión 31, tomo 3882, pág. 3946. 5 de septiembre de 1995.
[173] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2089. 5 de agosto de 1998. El paréntesis es nuestro.
[174] Art. 1 Ley 19.628. "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, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política. 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." BERTELSEN, Raúl. Datos personales: propiedad privada. Libre iniciativa particular y

artículo primero de la ley, el derecho a tratar datos personales dentro del marco legal, no estableciéndose, a lo menos formalmente, una clara entrega de titularidades o de derechos al titular de los datos que impliquen la posibilidad de control efectivo sobre su información personal. A este respecto, Christian Suárez, indica que "el proyecto parte de la base de reconocer a toda persona el derecho a recolectar, procesar, custodiar y transferir datos. Así lo expresa su artículo primero, agregando luego, en el inciso segundo, que reconoce este derecho con el propósito de proteger a las personas por el uso que terceros puedan hacer de sus datos personales", criticando tal técnica porque "nos lleva a situar su conceptualización jurídica, precisamente en el terreno menos oportuno, porque lo que las técnicas de protección de datos tratan de lograr no es ampliar las posibilidades jurídicas de individuos para recoger informaciones sobre los demás, sino que precisamente todo lo contrario"[175]. En este mismo sentido, aunque con otra connotación se pronuncia Raúl Bertelsen, quien indica a propósito de la ley en comento que: "Aunque no sea su objeto principal, puesto que la ley se denomina a sí misma de protección a la vida privada, y en el proyecto, de protección de datos de carácter personal, es indudable que contiene, aunque no lo sea en su totalidad, el marco legal que regula la actividad económica –esto es lucrativa- de tratamiento de datos"[176]. Asimismo, Felipe Vial indica que la ley reconoce en general la conveniencia social de los registros y bancos de datos y, de una u otra manera, se refiere a algunos registros que de paso legitima[177].

2.3. Ambito de aplicación de la ley

A efectos de revisar el ámbito de aplicación de la Ley 19.628, dividiremos su estudio en su alcance material u objetivo por una parte y subjetivo de otra.

---

respeto a la vida privada. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 115-129.

[175] SUÁREZ, Christian. Informática, vida privada y los proyectos chilenos sobre protección de datos. Revista Ius et Praxis. Universidad de Talca. 1997. Año 3. N° 1: 321-359.

[176] BERTELSEN, Raúl. Ib.

[177] Como ejemplos de estos bancos de datos menciona: los de información económica, bancaria, financiera y comercial que sirven de sustento al sistema crediticio; los de información de salud, que existen en apoyo del sistema de seguros de salud y del sistema provisional; los de información de contribuyentes en sustento del sistema impositivo del estado; los de información procesal y penal en apoyo del sistema procesal, penal y otras muchas instituciones y actividades en que como requisito se exige una conducta intachable de las personas; los de información civil, como base del sistema de identificación y determinación del estado civil de las personas; y los de información de las personas, sus ideologías, actividades, opiniones, etc., se justifica como relevante para la seguridad nacional."

2.3.1. Ambito de aplicación subjetivo

Nos ocuparemos de revisar en primer lugar, el ámbito de aplicación subjetivo de la ley, esto es, a quiénes y en qué términos se les aplica la Ley 19.628. De una parte, se encuentran aquellos que efectúan tratamiento de datos personales en registros o bancos de datos que según el artículo 1° inciso 1º de la ley pueden ser particulares u organismos públicos y de otra, los titulares de la información de naturaleza personal, encontrando además otra categoría de persona que resulta regulada en la ley, la del tercero receptor de datos personales.

a) Particulares dedicados al tratamiento de datos: son aquellos titulares de bancos o registros de datos que efectúan tratamiento de datos personales en forma particular o privada. La ley permite respecto de éstos que sean personas naturales o jurídicas.

b) Organismos públicos dedicados al tratamiento de datos: son aquellos organismos públicos titulares de bancos o registros de datos que efectúan tratamiento de datos personales. Con respecto a los órganos públicos, la misma ley en su artículo 2 letra k), se ha ocupado de definir qué se entiende por organismos públicos a efectos de la ley, adoptando un alcance amplio del concepto de órgano público, ya que comprende a las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política como los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, es decir, los Ministerios, las Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley. Cabe destacar que los organismos públicos que efectúan tratamiento de datos poseen una regulación especial en la Ley, que se encuentra en su Título IV "Del tratamiento de datos por organismos públicos"[178].

VIAL, Felipe. La ley 19.628 sobre protección de datos de carácter personal una visión general. En: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 23-37.

[178] Este Título consta de tres artículos: el 20 que establece los requisitos para que los organismos públicos puedan efectuar tratamiento de datos; el 21 que se refiere a al tratamiento de datos de naturaleza penal o criminal que efectúan los organismos públicos; y, finalmente el 23, que regula el

Tanto a los particulares como a los organismos públicos que se dedican a efectuar tratamiento de datos personales los denominaremos "titulares de registros o bancos de datos". Respecto a ambos tipos de titulares de registros o bancos de datos –privados y organismos públicos- cabe llamar la atención respecto del concepto establecido en el artículo 2 letra m) de la ley, que define al responsable del registro o banco de datos como "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". Creemos importante diferenciar entre los titulares de registros o bancos de datos –categoría que no se reconoce en forma expresa en la ley- y los responsables del registro o banco de datos, la distinción es una de género a especie: todos los responsables son titulares de registros o bancos de datos, ya que entendemos que efectúan tratamiento de datos ya sea en forma directa o a través de un tercero siendo esencial en todo caso que tomen las decisiones relacionadas con el tratamiento, sin embargo, no todos los que tratan datos son responsables de los registros o bancos de datos, porque puede suceder que ellos no tomen las decisiones respecto al tratamiento que efectúan, lo que usualmente ocurrirá en los casos en que existan de por medio contratos que externalicen la labor de tratamiento de datos, como por ejemplo puede ocurrir en contratos de prestación de servicios, outsourcing, mandato[179] u otros, en los cuales las decisiones respecto del tratamiento no las toma el que lo efectúa sino el que lo encarga a través de estos contratos y que en consecuencia es el responsable del fichero o banco de datos, lo que tiene especial importancia en materia de responsabilidad por el tratamiento de datos regulada en la Ley, ya que conforme al artículo 23 es la persona natural o jurídica privada o el organismo público responsable del tratamiento de datos, quien deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos.

c) El titular de los datos personales: El tercer sujeto normado por la Ley es el titular de los datos, que conforme al artículo 2 letra ñ) de la Ley es la persona natural a la que se refieren los datos de carácter personal. A su vez datos personales o de carácter personal son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables (artículo 2 letra f). Nuestra legislación opta por no comprender a las personas

---

Registro de los bancos de datos que llevan organismos públicos, tarea encomendada por el mismo artículo al Servicio de Registro Civil e Identificación.

[179] El artículo 8 de la Ley 19.628 permite que el tratamiento de datos se efectúe por mandato, en cuyo caso, se aplicarán las reglas generales. No obstante, establece que 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.

jurídicas, como sí lo han hecho otros ordenamientos, como por ejemplo, el argentino. Esto, debido a que nuestro legislador entiende que la intimidad, la vida privada son derechos que le corresponden en propiedad a las personas naturales y no a las jurídicas, a las cuales se les puede proteger por otras vías, como por ejemplo, por vía de reserva o secreto[180][181].

d) Terceros receptores de datos personales: Finalmente, como indicábamos, se encuentra una tercera categoría de personas que resulta normada indirectamente por la Ley 19.628, a saber, los terceros a los cuales se les comunican o transfieren datos personales[182]. Si bien no existe una regulación orgánica en la ley con respecto a estos sujetos[183], el artículo 5 que regula los procedimientos automatizados de transmisión o transferencia electrónica de datos personales, se refiere a ellos cuando indica que la responsabilidad derivada de un requerimiento de datos personales mediante una red electrónica será de quien la haga, es decir, del tercero a quien se le comunican los datos, agregando que éste sólo podrá utilizar los datos personales para los fines que motivaron la transmisión. Ahora bien, esta disposición no será aplicable cuando se trate de datos personales accesibles al público en general o cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

---

[180] A este respecto el Primer Informe de la Cámara de Diputados indicó que "En principio, el concepto de dato personal –y más aún el de intimidad- no es aplicable a las personas jurídicas y, por tanto, sus datos podrán ser siempre conocidos, pues prima el derecho a la información. Otra cosa será lo que se regule respecto del secreto comercial o industrial, por ejemplo". Informe de la Comisión de Constitución, Legislación y Justicia recaído en el proyecto de ley sobre protección a la vida privada. Cámara de Diputados. Segundo Trámite. Sesión 3, pág. 152. 04 de junio de 1996.

[181] No obstante lo anterior, cabe consignar que han existido algunas iniciativas legales en orden a incorporar a las personas jurídicas dentro del ámbito de aplicación de la ley, así por ejemplo, el Boletín 2422-07.

[182] Los comentarios que se efectúan en esta parte respecto a estos terceros, lo son en tanto, éstos son considerados receptores de datos personales en un proceso de comunicación de datos, y no en tanto pudieran constituir eventualmente y asimismo, titulares de registros o bancos de datos. Se encuentran en la primera situación, aquellas personas que solicitan la comunicación de datos, sin que efectúen con ellos un tratamiento que implique la creación de un registro o banco de datos como se le define en la ley, en cambio, se encontrarán en la segunda situación referida, todos aquellos que solicitan datos que luego tienen por objeto formar parte o ser almacenados en un registro o banco de datos.

[183] No existe tal tipo de regulación en la Ley 19.628, porque tampoco presenta este cuerpo normativo unas reglas armónicas en lo que respecta a la comunicación o transferencia de datos personales. Sólo el artículo 5° de la ley se refiere a este tema, a diferencia de lo que ocurre en derecho comparado, especialmente, en las legislaciones europeas, en las cuales, existen títulos especiales que regulan la formalidades y requisitos que debe cumplir la cesión, comunicación o transferencia de datos personales a terceros. Así, en España, el artículo 11 de la Ley Orgánica 15/99, de Protección de Datos de Carácter Personal; en Alemania, las secciones 15 y 16 del capítulo I de la Parte II de la Bundesdatenschutzgesetz (BDSG) de enero 2002 referida tratamiento de datos personales por órganos públicos y las secciones 29 y 30 del capítulo I de la Parte III referida al tratamiento de datos efectuado por particulares, en Italia el artículo 20 de la Legge N° 675, tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali de Diciembre 1996, establece los requisitos para la comunicación y difusión de los datos, dentro del capítulo III, Tratamiento de datos personales; sección IV Comunicación y difusión de datos.

2.3.2. Ambito de aplicación objetivo

El ámbito de aplicación material u objetivo de la Ley 19.628 se encuentra regulado básicamente en su artículo 1º inciso 1º que indica "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"[184].

De la norma trascrita se observa que el ámbito objetivo de la Ley se encuentra determinado por el concepto de tratamiento de datos personales, que la Ley en el artículo 2 letra o) ha definido como "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". De la definición legal destaca que se trata de un concepto amplio y genérico[185], dada la utilización del vocablo "cualquier" y de la frase "o utilizarlos en cualquier otra forma" y que comprende diversas acciones de carácter técnico a título ilustrativo[186]. La amplitud de la definición conlleva que la Ley se aplique a cualquier operación que permita utilizar datos personales de alguna forma. Lo anterior, se ve reforzado por que la Ley se aplica a cualquier tipo de tratamiento de datos personales, ya sea éste automatizado o manual.

Este concepto de tratamiento de datos debemos relacionarlo necesariamente con el de registro o banco de datos, definido por la Ley en el artículo 2 letra m) como "el conjunto organizado de datos de carácter personal, sea automatizado o no, y cualquiera sea la forma o

[184] Se indica, además, una excepción en el sentido de que aquél tratamiento de datos personales que se efectúe en razón de ejercicio de las libertades de emitir opinión y de informar, se regulará por la ley a que se refiere el artículo 19 número 12 de la Constitución Política, que según el texto constitucional ha de ser de quórum calificado, esta ley fue publicada en el Diario Oficial con fecha 04 de junio de 2001 bajo el número 19.733 y es conocida como Ley de Prensa.

[185] Como indica Felipe Vial "el largo listado de operaciones que contempla la definición legal, revela el propósito del legislador de definir un concepto lo más amplio posible a este respecto". VIAL, F. op.cit. pág.24.

[186] "La Comisión Mixta mantuvo la idea de enunciar las diferentes actividades susceptibles de ser realizadas, ya que abarcan prácticamente todas las situaciones de tratamiento de datos... Al mismo tiempo, creyó útil reforzar su carácter simplemente ejemplar, añadiendo una referencia de orden general que especifica que el tratamiento de datos considera la utilización de los mismos en cualquier forma, para así cubrir cualquier omisión en que se pudiera haber incurrido". Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2096. 05 de agosto de 1998.

modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos."

De estos dos conceptos básicos queda de manifiesto el ámbito material de la Ley, comprensivo tanto de las operaciones de tratamiento automatizado de datos como manual de estos mismos, estableciendo como elemento esencial la circunstancia de que tal tratamiento permita relacionar los datos personales entre sí, conformando un conjunto organizado de ellos.

2.4. La autorización o consentimiento

Como ya revisáramos en el Capítulo I de esta tesis, uno de los principios fundamentales que se reconocen en materia de tratamiento de datos personales es el denominado principio del consentimiento del afectado, así lo reconoce Ana Herrán[187] cuando señala que "No hará falta insistir en la importancia que el derecho del consentimiento alcanza en la protección de datos personales, ya que a partir del reconocimiento de un derecho a consentir el tratamiento de los datos se estructura y organiza la autodeterminación informativa o la facultad de los interesados de establecer y decidir sobre el tratamiento de la información que les concierne". Este principio recibe reconocimiento con mayor o menor fuerza en todas las legislaciones protectoras de datos, como asimismo, en las declaraciones de organismos internacionales sobre los principios rectores que deben estar presentes en materia de tratamiento de datos personales.

Al referirnos a continuación al consentimiento o autorización en la Ley 19.628, lo haremos desde las características que éste presenta a propósito de los siguientes elementos: definición o contenido, extensión, excepciones y revocación.

[187] HERRÁN, A. op.cit. pág. 220.

2.4.1. Definición o contenido

A diferencia de algunas legislaciones extranjeras[188], la Ley 19.628 no define la autorización o consentimiento del titular de los datos, limitándose a señalar en su artículo 4 que "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".

En el ámbito del derecho comparado, especialmente, el europeo se indican ciertas características que debe cumplir el consentimiento del titular de los datos[189], las cuales se pueden resumir en que éste debe ser: manifestado, libre, específico e informado.

Que el consentimiento sea manifestado quiere decir que se requiere que éste sea declarado, ya sea en forma tácita o expresa[190]. En este punto, nuestra ley no da cabida a interpretaciones sobre la posibilidad de una autorización tácita para efectuar tratamiento de datos

---

[188] La Ley Orgánica de Protección de Datos española define el consentimiento en su artículo 3 letra h) en los siguientes términos: "Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de los datos personales que le conciernen". Asimismo, el artículo 2 de la ley 2.472 de protección de las personas respecto al tratamiento de datos de carácter personal de 26 de marzo de 1997 de Grecia, define el consentimiento como "toda indicación libremente prestada, explícita y específica, por la que el titular del dato expresamente y plenamente consciente, es decir, informado, consiente a que los datos relativos a él sean tratados". También el artículo 3 letra h) de la ley 67/98 de 26 de octubre de 1998 sobre la protección de datos personales de Portugal define el consentimiento del titular de los datos como cualquier manifestación de voluntad, libre, específica e informada, por la cual el titular acepta que sus datos personales sean objeto de tratamiento. Todas estas legislaciones se inspiran en lo señalado en la Directiva Europea sobre la materia, la cual en su artículo 2 letra h), define el consentimiento del interesado como toda manifestación de voluntad, libre, específica e informada, mediante la cual el interesado consienta el tratamiento de datos que le conciernan.

[189] Ver nota al pie anterior.

[190] Algunos autores como Emilio del Peso, indican que cabe la posibilidad que el consentimiento en materia de protección de datos, pueda asumir tres formas: expreso, tácito y presunto, ya que en ningún artículo de la ley (la LOPD española) se dice cuántos tipos de consentimiento existen, pero unas veces habla de consentimiento expreso escrito, otras de consentimiento expreso y otras simplemente de consentimiento. Expreso es el que se manifiesta mediante un acto positivo o declarativo de la voluntad. Puede ser de forma oral o escrita. Tácito es el que se produce cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume como acto de aceptación. Presunto es el que no se deduce ni de una declaración ni de un acto de silencio positivo, sino que de un comportamiento o conducta que implica aceptación. DEL PESO, Emilio. Protección de datos. 2000. La nueva LORTAD. Madrid, Ediciones Díaz de Santos. 441p.

personales, ya que exige que el titular consienta expresamente en ello y que lo haga, además, por escrito. Respecto al momento en que debe ser prestada la autorización en tanto manifestación de voluntad, la Ley guarda silencio, lo que ha llevado a un autor nacional, Renato Jijena, a señalar que "como nada se dice, creemos que la autorización podrá ser otorgada antes o después de iniciado el procesamiento con lo cual tendría lugar la ratificación"[191]. No compartimos este criterio por dos razones, la primera es de orden lógico, si se permitiera la figura de la ratificación en la práctica la exigencia de la autorización del titular para efectuar tratamiento de datos no operaría, y estaríamos, entonces, en presencia de un sistema normativo en el cual la regla general es poder efectuar libremente tratamiento de datos personales, funcionando en este sistema el consentimiento ex – post, ya sea para ratificar o bien para impedir el tratamiento de datos, en los casos en que fuera necesario el consentimiento del titular conforme a la ley[192]; la segunda razón es de texto, el inciso primero del artículo 4 de la ley es claro cuando indica que "el tratamiento de datos personales sólo puede efectuarse….cuando el titular consienta expresamente en ello", por lo tanto, y en contrario, si el titular de los datos no consiente expresamente en ello, el que pretende efectuar tratamiento de sus datos personales no puede siquiera dar comienzo al proceso de tratamiento, ya que no cuenta con la autorización inicial del titular de los datos exigida por la norma.

El consentimiento libre dice relación con la ausencia de vicios del consentimiento[193]. La ley 19.628 no señala, a diferencia de lo que ocurre en la mayoría de las legislaciones europeas, que la autorización del titular de los datos deba ser libre, lo que en nuestra perspectiva es

[191] JIJENA, Renato. 2001. La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 85-111. pág 101.

[192] Este sistema es el que los autores norteamericanos denominan *opt-out*. Para un concepto ver el Glosario. Además, en la historia de la ley quedó plasmado el parecer de la Comisión de Constitución, Legislación y Justicia en este orden de cosas frente al requerimiento efectuado por la Asociación de Marketing Directo, que sugirió establecer, como forma de hacer compatibles la protección de los datos personales con el desarrollo de la actividad comercial, el mecanismo de la autoexclusión, en virtud del cual se reconoce a cada individuo el derecho de requerir de parte de quien efectúe tratamiento de sus datos que deje de hacerlo. La referida Comisión señaló al respecto: "…siendo dicha persona el titular de los datos…no se le brindaría la protección que anuncia la denominación de este cuerpo legal si se sustituye ese mecanismo por el de la autoexclusión, ya que ello implicaría que datos respecto de los cuales corresponde al titular resolver si los da a conocer o no, o si permite que sean objeto de tratamiento, pudiesen ser utilizados incluso sin su conocimiento. Ello obligaría al particular cuyos datos se encuentren almacenados a estar permanentemente consultando sobre la inclusión de sus datos en los bancos, lo cual resulta, a todas luces, imposible de poner en la práctica, o, al menos constituiría una carga gravosa e injustificada, atendido que la titularidad de los datos le pertenece". Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2102. 05 de agosto de 1998.

[193] MARTÍNEZ, Carlos. 2002. Protección de datos de carácter personal. El consentimiento en entidades financieras. Asociación Nacional de Establecimientos Financieros de Crédito. 173p. pág 62.

acertado, ya que no resulta necesario establecer este requisito del consentimiento en forma expresa, ya que la autorización en tanto manifestación de voluntad para que produzca sus plenos efectos debe cumplir con los requisitos que se presentan como generales en nuestro ordenamiento, dentro de los cuales, nuestro Código Civil indica al consentimiento libre de vicios[194].

Que el consentimiento sea específico "hace referencia con claridad a que el consentimiento debe recogerse para un determinado tratamiento. Se une por tanto el problema del principio del consentimiento con el principio de la finalidad"[195]. Nuevamente, si bien la Ley 19.628 no se refiere en forma expresa a este requisito del consentimiento, podemos observar que éste se encuentra recogido con mediana intensidad cuando se establece la obligación en el inciso segundo del artículo 4 para el que pretende efectuar tratamiento de datos de informar al titular de ellos el propósito del almacenamiento de sus datos[196] y cuando el artículo 9 de la ley indica que "Los datos personales debe utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público".

El consentimiento informado requiere que se cumpla con lo señalado en la legislación respectiva en cuanto a los contenidos que deben ser notificados al titular de los datos cuando éste presta su consentimiento. A este respecto, nuestra ley es menos exigente que las legislaciones existentes en otros países[197], ya que el inciso segundo de su artículo 4 sólo obliga a informar al titular de los datos respecto del propósito del almacenamiento de los datos personales y su posible comunicación al público, es decir, conforme al artículo 2 letra c) si los datos personales

[194] CHILE. CÓDIGO CIVIL. Artículo 1445 "Para que una persona se obligue a otra por un acto o declaración de voluntad es necesario: 1.- que sea legalmente capaz; 2.- que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio; 3.- que recaiga sobre un objeto lícito; 4.- que tenga una causa lícita".
[195] MARTÍNEZ, Carlos. op.cit. pág. 67.
[196] Respecto a este requisito, creemos que éste no se cumple si se utilizan fórmulas genéricas que no indican una finalidad en el tratamiento específica, como por ejemplo, indicar que se almacenarán los datos personales con el objeto de efectuar tratamiento de ellos.
[197] Por ejemplo, la Ley Orgánica Española de Protección de Datos (LOPD) señala en su artículo 5 número 1 que: "Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante."

recogidos se darán a conocer a personas distintas del titular, sean determinadas o indeterminadas.

Finalmente, cabe preguntarse acá si es posible prestar autorizaciones generales para el tratamiento de datos, esto es, no para un tratamiento específico que efectúe un determinado titular de banco de datos, sino que en forma genérica. Creemos que dada la normativa vigente y, en particular, en razón del artículo 4 de la Ley 19.628, esta clase de autorizaciones generales no debieran surtir efectos, ya que no resulta viable cumplir con el consentimiento informado, pues en este tipo de autorizaciones, la información al titular de los datos respecto de la finalidad del tratamiento y su comunicación al público no podrá efectuarse por no tener certeza respecto de estas materias.

2.4.2 Extensión

Llamamos extensión de la autorización o consentimiento, a su exigencia tanto para el tratamiento de datos personales, como para la transferencia de ellos a terceros. En el ámbito comparado, algunas legislaciones no sólo han señalado como regla general el consentimiento para efectuar tratamiento de datos, sino que también, específicamente para la cesión de ellos a terceros[198]. Nuestro legislador optó por no seguir esta tendencia de manera que no se exige autorización para la comunicación o transferencia de datos a terceros[199].

2.4.3 Excepciones

El artículo 4 de la Ley en su inciso primero indica el principio general existente en materia de protección de datos personales, tanto en nuestro país como en el ámbito internacional, cual es que el tratamiento de los datos personales sólo puede efectuarse cuando la Ley 19.628 u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. Por lo tanto, las excepciones al consentimiento por parte del titular de los datos, sólo pueden ser establecidas por normas de rango legal, ya sea aquellas que se señalen en la misma Ley 19.628 o en otra

[198] Así ocurre con las legislaciones argentina, española, italiana, entre otras.
[199] La cesión y transferencia de datos, será estudiada con profundidad en el próximo acápite.

norma de igual jerarquía. Las excepciones a la autorización del titular de los datos que se indican en la propia Ley 19.628 suelen ser agrupadas en cuatro[200][201]:

i) Cuando los datos personales provienen o se recolectan de fuentes accesibles al público, cuando:

a) Sean datos de carácter económico, financiero, bancario o comercial;

b) Sean datos que 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,

c) Sean datos necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios (artículo 4).

ii) Cuando se trate del tratamiento de datos personales que efectúen personas jurídicas privadas, siempre que se trate copulativamente:

a) De datos personales para uso exclusivo de las personas jurídicas privadas, de sus asociados y de las entidades a que están afiliadas.

b) El tratamiento se efectúe con fines estadísticos, de tarificación u otros de beneficio general de los mismos (artículo 4).

iii) En los casos de tratamiento de datos personales que efectúen organismos públicos respecto de materias de su competencia (artículo 20).

iv) Cuando el tratamiento de datos personales se efectúe para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (artículo 10).

Respecto a otras disposiciones legales que constituyan una excepción al consentimiento del titular de los datos, podemos encontrar disposiciones que en forma expresa autorizan el tratamiento de datos, como también normas que implican tácitamente una autorización para efectuar el tratamiento de los datos sin consentimiento de la persona a la cual éstos conciernen. Ejemplo del primer tipo de disposición encontramos la ley que crea el Consejo Nacional de la

[200] VIAL, Felipe. op.cit. pág 27.

Cultura y las Artes y el Fondo Nacional de Desarrollo Cultural y las Artes, en la cual su artículo 3 Nº 12 señala como función del consejo: "Desarrollar y operar un sistema nacional y regional de información cultural de carácter público. Para la operación del sistema nacional y regional de información cultural, a que hace referencia este numeral, el Consejo podrá crear un banco de datos personales, de aquellos señalados en la Ley 19.628"[202]. Respecto a autorizaciones tácitas para efectuar tratamiento de datos, el Código del Trabajo[203] establece en su artículo 10 las estipulaciones que debe contener el contrato de trabajo dentro de las cuales encontramos información personal del trabajador, como por ejemplo, su individualización, nacionalidad, fecha de nacimiento, ingreso. Podemos señalar que, en este caso, al exigir la ley que el contrato de trabajo contenga datos personales del trabajador, el empleador se encuentra autorizado por una disposición legal a efectuar tratamiento de estos datos personales, sin necesidad, consecuentemente de una autorización expresa por parte del empleado, debiendo, en todo caso, el empleador cumplir con las normas que se indican en la Ley 19.628, respecto a la finalidad del tratamiento, seguridad, calidad de los datos, etc.

2.4.4. Revocación.

La ley contempla la posibilidad para el titular de los datos de revocar la autorización que ha otorgado para que se efectúe tratamiento de su información personal; el inciso 4 del artículo 4 prescribe: "La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito". Respecto a la norma citada, cabe preguntarse qué significa que la revocación de la autorización no tenga efectos retroactivos: la historia de la ley y la jurisprudencia no se han pronunciado, en doctrina nacional Alberto Cerda ha indicado que la irretroactividad de la revocación implica la no privación de legitimidad al tratamiento de que fueron objeto los datos personales con antelación[204], es decir, el resultado de la revocación es la imposibilidad para el autorizado de seguir efectuando tratamiento de los datos personales a partir del momento en que ésta le es comunicada por escrito por el titular de los datos respectivo,

---

[201] Las excepciones a la autorización del titular, serán estudiadas con profanidad cuando más adelante nos refiramos a las distintas categorías de datos reconocidas en la Ley 19.628.
[202] CHILE. Ley N° 19.891. 2003. Crea el consejo nacional de la cultura y las artes y el fondo nacional de desarrollo cultural y las artes.
[203] Chile. D.F.L.1. 2003. Fija el texto refundido, coordinado y sistematizado del Código del Trabajo.
[204] CERDA, Alberto. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. 2003. Tesis para optar al grado de magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho. 260p.

siendo legítimas en consecuencia, las operaciones efectuadas sobre los datos con anterioridad a la referida revocación, incluyendo eventuales cesiones a terceros de los datos, y es con respecto a este punto que se produce el siguiente cuestionamiento ¿La revocación de la autorización produce efectos respecto del tercero al cual legítimamente se le cedieron los datos con anterioridad a ella? Para responder esta pregunta se debe determinar si esta revocación implica que los datos en cuestión se deban eliminar o cancelar, lo que creemos es así ya que la no eliminación de los datos implica en la práctica que se sigue efectuando tratamiento de ellos, dada la amplitud con que la ley define tratamiento de datos [205]. Asimismo, cabe tener presente que el titular de los datos puede ejercer junto con la revocación el derecho de cancelación o eliminación que le otorga el inciso 4 del artículo 12 de la ley[206]. Por lo anterior, es claro que en ambos casos de revocación, esto es, si hay o no junto con la revocación una solicitud expresa de cancelación se debe aplicar lo señalado en el inciso final del artículo 12 de la Ley el cual indica que "Si los datos 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 fuere 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", la finalidad de este aviso, aun cuando la ley no lo diga en forma expresa, no puede ser otra que el tercero al cual se le han cedido o comunicado los datos sepa que no puede seguir efectuado tratamiento de los datos que fueron eliminados, es decir, que la revocación de la autorización efectivamente le obliga[207].

[205] "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." Art. 2 letra o) Ley 19.628.

[206] Art. 12 Ley 19.628 inciso 4: "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."

[207] Sin perjuicio de lo señalado, reconocemos que podría argüirse con cierto fundamento que al no estar regulada en nuestra legislación la figura de la autorización del titular de los datos en la cesión de ellos y al ser legítimo el tratamiento de datos efectuado con antelación a la revocación –incluida la cesión- la respuesta a la pregunta que efectuamos es negativa, es decir, este tercero podría legítimamente seguir tratando los datos personales cedidos no obstante la revocación.

2.5. La comunicación o transferencia de datos a terceros

La comunicación, transferencia, transmisión o cesión[208] de datos personales puede efectuarse a través de las fronteras territoriales de los países, en cuyo caso se denomina tanto por la legislación como por la doctrina "transmisión transfronteriza de datos personales", o bien puede efectuarse en forma local, es decir, dentro de los límites de un determinado país. Como señala Osvaldo Gozaíni[209] "La información personal que se redistribuye tiene dos radios de acción. Puede hacerse para un mercado local y centrar en las normas internas su cobertura legal, o transmitirse hacia el exterior, en cuyo caso el traslado de esa información está condicionada a que exista en el país donde habrá de alojarse una protección equivalente a la del lugar donde el dato se origina". A partir de esta clasificación revisaremos cómo la Ley 19.628 regula la comunicación de datos.

2.5.1. Comunicación o transferencia internacional

La transferencia internacional de datos personales[210], se encuentra regulada en un importante porcentaje de aquellos ordenamientos jurídicos que poseen legislaciones protectoras de datos personales, como asimismo, se refieren a ella distintos organismos internacionales. La norma general respecto a este tipo de comunicación es que las normativas exijan que el país al cual se transfieren los datos tenga una protección equivalente al país de origen o a lo menos adecuada, lo que supone que el Estado al que se transfiere la información tenga un régimen normativo parecido al que se cuenta en el lugar donde está asentado el archivo de remisión[211], reconociendo, en todo caso, que no pueden establecerse límites injustificados en el libre flujo de los datos personales.

---

[208] Estos términos, en general, son utilizados como sinónimos en las distintas legislaciones protectoras de datos, como asimismo, por la doctrina, aun cuando desde un punto de vista técnico pueden establecerse ciertas diferencias.
[209] GOZAINI, Osvaldo. op.cit. pág. 315.
[210] El Convenio 108 del Conejo de Europa define este tipo de comunicación como la transmisión a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento. CONSEJO DE EUROPA. 1981. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Agosto 1981.
[211] GOZAINI, Osvaldo. op.cit. pág. 323.

La Asamblea General de las Naciones Unidas prefiere la libertad de circulación de los datos cuando no se advierte una clara violación a la vida privada de los titulares de los datos, así indica dentro de los principios rectores para la reglamentación de los ficheros computarizados de datos personales que "Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, y sólo en la medida en que así lo exija la protección a la vida privada."[212] Un criterio similar al de la ONU asume la OCDE cuando indica que "Los países miembros deberán abstenerse de restringir el intercambio transfronterizo de datos personales con otros países miembros, excepto cuando el país receptor todavía no observe de forma sustancial estas directrices o cuando la reexportación de tales datos burle la legislación nacional sobre privacidad."[213] La Directiva Europea vigente en la materia, parece ser más exigente que los criterios recién mencionados, cuando el artículo 25 dispone como principio general que los Estados miembros dispondrán que la transferencia, a un tercer país, de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente puede efectuarse cuando, el tercer país de que se trate garantice un nivel de protección adecuado. El nivel de protección que ofrece un tercer país, según el apartado 2 del artículo 25 de esta directiva, se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; y en particular, se tomará en consideración: la naturaleza de los datos; la finalidad y duración del tratamiento o de los tratamientos previstos; el país de origen y el país de destino final; y, las normas de derecho, generales o sectoriales, vigentes en el tercer país de que se trate, así como las medidas de seguridad en vigor en dichos países.

Diversas legislaciones europeas, y la argentina en nuestro ámbito han adoptado reglas que recogen los principios recién referidos. Nuestra legislación, sin embargo, decidió no regular

[212] NACIONES UNIDAS. 1990. Resolución 45/95 de la Asamblea General sobre Principios rectores para la reglamentación de los ficheros computarizados de datos personales. Diciembre 1990.
[213] ORGANIZACION PARA LA COOPERACION Y EL DESARROLLO ECONOMICOS. 1980. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Septiembre 1980.

la transferencia internacional de datos, el Senado rechazó el precepto[214] que se refería a esta materia debido a que consideró que la regulación de la transferencia internacional de datos corresponde ser efectuada por tratados internacionales sobre la materia, evitando de esa forma anticipar en la ley que se tramitaba criterios que puede que no correspondan a los que se pacten internacionalmente, y las dificultades de interpretación, en cada caso, que pueda presentar la expresión garantías análogas[215]. De esta manera, actualmente la transferencia internacional de datos se encuentra permitida en nuestro país, siempre y cuando se cumplan las disposiciones generales establecidas en el texto legal[216]. Por último, cabe señalar a este respecto que la ausencia de regulación en esta materia, puede entrabar cualquier transferencia de datos personales que se pretenda efectuar con algún país de la Unión Europea, ya que como señala Pablo Palazzi "una transferencia de datos a Chile no aseguraría -salvo las estipulaciones contractuales del caso específico concreto- una eventual transferencia a un tercer país que no tiene legislación adecuada."[217]

2.5.2. Comunicación o transferencia local

Las implicancias de la posibilidad de comunicación de datos a terceros y cómo se efectúa es un tema central en cualquier legislación protectora de datos personales, ya que la transferencia de datos constituye la forma a través de la cual las personas toman conocimiento de los datos personales de terceros. No obstante la importancia de la comunicación de los datos y del establecimiento de normas claras a su respecto, nuestra ley presenta una regulación bastante

[214] El artículo 23 del proyecto que fue rechazado por el Senado prohibía a los responsables de bancos de datos personales transmitir datos personales desde países o con destino a países cuya legislación no ofrezca garantías análogas a las previstas en esta ley. Se exceptúan las trasferencias internacionales de créditos, las transferencias de información para los efectos de prestar colaboración que resulte de la aplicación de tratados o convenios internacionales en que el estado de Chile sea parte".

[215] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2120. 05 de agosto de 1998. El artículo 23 rechazado consignaba. "Prohíbese a los responsables de bancos de datos personales transmitir datos personales desde países o con destino a países cuya legislación no ofrezca garantías análoga a las previstas en esta ley.
Se exceptúan las transferencias internacionales de créditos, las transferencias de información para los efectos de prestar colaboración a las autoridades judiciales y policiales internacionales, así como cualquier otra transferencia que resulte de la aplicación de tratados o convenios internacionales en que el Estado de Chile sea parte".
Del transcrito artículo sólo se recogió en el texto definitivo de la ley- en el artículo 5 inciso final- que las restricciones o requisitos señalados en el referido artículo para la transmisión de datos, no aplicarán cuando se transmitan datos personales a organizaciones internacionales en cumplimiento a lo dispuesto en tratados y convenios vigentes.

[216] MAGLIONA, Claudio. Habeas Data y Protección de Datos Personales en Chile. [en línea] <http://www.adi.cl/pdf/magliona2.pdf >[consulta: 12 enero 2005]

[217] PALAZZI, Pablo. op.cit. pág. 186.

exigua de esta operación, no exigiendo ni el consentimiento ni el conocimiento por parte del titular de los datos sobre la comunicación a terceros de sus datos. La falta de exigencia legal de consentimiento, o al menos, de conocimiento por parte del titular de los datos sobre la comunicación de su información a terceros, trae importantes consecuencias sobre la posibilidad de control efectivo del titular de los datos sobre su información personal, ya que si bien, en un comienzo éste puede tener claridad respecto de quién está efectuando tratamiento de sus datos personales – y poder así ejercer los derechos que le entrega la ley- al poder comunicarse esos datos a un tercero que el titular de datos desconoce (por la falta de consentimiento y/o comunicación), éste pierde en esta instancia toda posibilidad de control, además, este tercero puede perseguir una finalidad distinta de la que motivó y legitimó la recolección de los datos originalmente[218].

Ya analizando la regulación que la Ley 19.628 efectúa de la comunicación de datos a nivel local, debemos referirnos en primer lugar a la conceptualización que de ella hace el artículo 2 letra c): "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". La definición legal es bastante amplia por lo que debemos entender que constituye comunicación, cualquier operación que implique poner en conocimiento los datos personales a un tercero, ya sea en forma gratuita u onerosa; ya sea a través de la entrega de un soporte físico o a través del envío de los registros en formato digital por una red o por último permitiendo la sola visualización; ya sea permitiendo que la persona a la cual se comunican los datos efectúe a su vez tratamiento de dichos datos o no.

Esta amplitud del concepto se hace mayor aun con la definición que de tratamiento de datos efectúa la Ley 19.628 en su artículo 2 letra o), ya que dentro de las operaciones que implican efectuar tal tratamiento encontramos algunas que se pueden confundir, o que, a lo menos, pueden encontrarse dentro del mismo plano que la comunicación, así se refiere a: "interconectar, comunicar, ceder, transferir, transmitir … datos de carácter personal." Por de pronto, la ley hace sinónimos a la comunicación con la transmisión. La transferencia, se entiende que se produce cuando se comunican datos en forma transfronteriza. La interconexión, se

[218] Este tema volverá ser analizado en el Capítulo IV de esta tesis, cuando se plantee un nuevo modelo de protección de datos.

entiende como la acción de conectar entre sí aparatos o sistemas, de forma que entre ellos pueda fluir algo material o inmaterial (en este caso datos personales), finalmente entenderemos por cesión, cuando se entrega a otro la titularidad sobre los bancos o registros de datos personales, ya sea a título gratuito u oneroso, como por ejemplo, cuando se vende una base de datos.

El artículo 5 de la Ley regula en forma parcial la comunicación o transmisión de datos a terceros, efectuando un tratamiento diferenciado según se trate de un procedimiento automatizado de transmisión de datos o un requerimiento de datos personales a través de una red electrónica[219]. De esta manera, a toda comunicación de datos que no se pueda encasillar dentro de alguna de estas categorías, como por ejemplo, una comunicación de datos a través de la entrega material de un soporte físico no se le aplica lo señalado en este artículo. Veremos a continuación las reglas que se establecen en la norma en comento a fin de garantizar los derechos de los titulares de datos cuando se comunican sus datos a terceros.

2.5.2.1. Procedimiento automatizado de transmisión de datos

El inciso primero del artículo 5 dispone: "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".

Esta norma permite a quien efectúe tratamiento de datos que transmita la información personal a terceros distintos del titular utilizando métodos automatizados, es decir, que funcionan en todo o en partes por sí solos, sin intervención inmediata del ser humano[220], siempre que se cumplan los siguientes requisitos mínimos:

a.- Se cautelen los derechos de los titulares.

---

[219] Respecto a esta distinción cabe señalar que la relación que se presenta entre estas dos categorías es de género a especie, ya que todo requerimiento de datos efectuado a través de una red electrónica implica un procedimiento automatizado de transmisión, pero no todo procedimiento automatizado de transmisión requiere la existencia de un requerimiento de datos.

[220] DICCIONARIO DE LA LENGUA ESPAÑOLA. Vigésima segunda edición [en línea] < http://www.rae.es/> [consulta: 18 marzo 2005]

Lo que es una aplicación del principio general establecido en el inciso segundo del artículo 1 de la Ley[221].

b.- La transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Respecto de este requisito cabe señalar que nada dice en relación con que esta transmisión deba guardar relación con la finalidad con que fueron recabados los datos personales que se transmiten (principio de la finalidad en el tratamiento), sino que con la finalidad de los organismos participantes en la transmisión, conceptos que son claramente distintos.

2.5.2.2 Requerimiento de datos personales a través de una red electrónica

Luego, el artículo 5 en su inciso 2 establece a propósito de requerimientos de datos personales a través de redes electrónicas, es decir, a través de un conjunto de computadores o de equipos informáticos conectados entre sí que pueden intercambiar información[222], ciertas responsabilidades tanto para el que efectúa el requerimiento como para el responsable del banco de datos respectivo. Así, éste último deberá dejar constancia de:

a) La individualización del requirente;
b) El motivo y el propósito del requerimiento, y
c) El tipo de datos que se transmiten.

Asimismo, el responsable del banco de datos debe evaluar la admisibilidad del requerimiento. De su parte, el que efectúa la petición de transmisión de datos es responsable de dicha petición.

[221] Art. 1 inciso 2 Ley 19.628: "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."
[222] DICCIONARIO DE LA LENGUA ESPAÑOLA. Vigésima segunda edición [en línea] < http://www.rae.es/> [consulta: 18 marzo 2005]

Por último, se establecen en este artículo, reglas comunes a los dos tipos de transmisión de datos analizadas. En primer lugar, se señala que el receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión. En la tramitación del proyecto de ley, la Comisión de Constitución, Legislación y Justicia y Reglamento señaló en su informe respecto de esta obligación, que: "La Comisión compartió los objetivos de la norma, de consagrar todos los resguardos necesarios para la transmisión automática de los datos personales, sobre todo para prevenir que los datos que se comunican sean usados para un fin distinto de aquel que se tuvo en vista al proporcionarlos."[223] Cabe observar respecto de esta obligación, que nuevamente pareciera que el legislador aplica el principio de finalidad, ya que hace referencia al respeto de los fines que se tuvieron presentes al momento de efectuar la transmisión de los datos, sin embargo no es así, ya que guarda silencio en relación al respeto que se debiera tener, en aplicación del referido principio, a la finalidad con que se recabaron los datos que se transmiten. En segundo lugar, se señala que estas normas no se aplicarán cuando se trate de datos personales accesibles al público en general, esto es de acceso no restringido o reservado a los solicitantes ni cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en tratados y convenios vigentes, ya que en estos casos regirá lo señalado en los referidos instrumentos internacionales.

2.6. Categorías de datos reconocidas en la Ley 19.628

Los datos personales[224] o datos de carácter personal son, conforme la definición del artículo 2 letra f) de la Ley 19.628, "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables". Como se puede observar, se trata de una definición bastante amplia que abarca cualquier información que se refiera a un sujeto identificado o susceptible de serlo[225]. Todos los datos que regula la ley, salvo los denominados

[223] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2107. 05 de agosto de 1998.

[224] Podemos concluir de la lectura de la Ley 19.628 que existe una primera gran clasificación de los datos entre datos personales y datos estadísticos. Los datos estadísticos son definidos en el artículo 2 letra e) como aquellos, que en su origen, o como consecuencia de su tratamiento -a través de un procedimiento de disociación de datos- no pueden ser asociados a un titular identificado o identificable. Su característica fundamental es que no están protegidos, al ser imposible asociarlos a una persona determinada o determinable, por lo que no son considerados en la clasificación propuesta al no constituir datos personales.

[225] Como ya mencionáramos anteriormente, persona identificable es toda aquella, cuya identidad puede determinarse, ya sea de forma directa o indirecta, a través de uno ó más elementos de su identidad. A este respecto el Primer Informe de la Cámara de Diputados indicó que "Identificable significa que se puede identificar fácilmente, excluyendo la identificación por medios complejos. Por eso, no se

datos estadísticos[226], calzan dentro de este concepto de datos personales, sin embargo, la regulación que la ley efectúa de esta gran categoría de datos –la de datos personales- no es símil. El criterio que se utilizará en esta tesis para categorizar los distintos tipos de datos personales, está determinado por el mayor o menor grado de control que es otorgado por la Ley al titular de los datos respecto a la información que le concierne, es decir, conforme la intensidad con que se presenta la asignación de titularidades al referido titular, según el tipo de dato personal de que se trate. Para ello, tomamos en cuenta la necesidad que tiene el titular del registro o banco de datos de solicitar autorización al titular de los datos personales si pretende efectuar tratamiento de sus datos. A este respecto, como ya mencionáramos, la regla general establecida en el artículo 4 de la ley indica que el tratamiento de datos personales sólo se puede efectuar cuando existe una autorización legal para ello, ya se encuentre contemplada en la misma Ley 19.628 o en otra ley, o bien, exista una autorización previa y por escrito por parte del titular de los datos. Los distintos tipos de datos que se pueden reconocer en la normativa, en base al criterio expuesto, son los siguientes:

2.6.1. Datos personales provenientes de fuentes accesibles al público.

Este tipo de datos se caracteriza porque se pueden tratar sin autorización del titular, en tres hipótesis taxativas y alternativas que contempla la ley en su artículo 4 inciso quinto[227], a saber:

a) Cuando sean datos de carácter económico, financiero, bancario o comercial, o;

---

consideran inidentificables los datos despersonalizados, como los que se obtienen de las encuestas. Pero se considera identificable toda persona cuya identidad pueda determinarse mediante un número de identificación u otra información similar". Informe de la Comisión de Constitución, Legislación y Justicia recaído en el proyecto de ley sobre protección a la vida privada. Segundo Trámite. Cámara de Diputados. Sesión 3, pág. 152. 04 de junio de 1996.

[226] Ver nota anterior.

[227] Art. 4 Ley 19.628 inciso 5: "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". No obstante existe consenso tanto en la doctrina como en la jurisprudencia, respecto a que el inciso transcrito se refiere a tres hipótesis distintas de datos contenidos en fuentes accesibles al público y no a requisitos copulativos de procedencia de la excepción (no se requiere autorización del titular de los datos), cabe mencionar que de en una primera lectura y dado lo confuso de la redacción, podría llegar a concluirse que se trata de la regulación de tres requisitos copulativos que deben cumplir los datos contenidos en fuentes accesibles al público, para que proceda la excepción.

b) Cuando sean datos que 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;

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

Constituye, pues, este tipo de datos una excepción al principio general que exige la autorización previa del titular de los datos para efectuar su tratamiento. Dada la importancia práctica que reviste la excepción, nos referiremos a continuación *in extenso* a ella.

2.6.1.1. Derecho comparado

En derecho comparado esta excepción se encuentra establecida en algunas de las leyes de protección de datos europeas y algunas latinoamericanas que han tomado como fuentes las referidas leyes europeas. En Europa, las leyes española e italiana establecen el concepto de fuentes accesibles al público como excepción al principio general del consentimiento del titular, y la alemana e inglesa utilizan el concepto como excepción a otros principios o reglas, lo anterior no obstante la Directiva Europea sobre la materia[228], no se haya referido a ellas. Así, la Ley Orgánica de Protección de Datos española (LOPD)[229] define a las fuentes accesibles al público en su artículo 3 letra j), como "Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación", estableciendo en el artículo 6.2 que no será necesario el consentimiento del afectado, es decir, del titular de los datos, cuando "los datos figuren en fuentes accesibles al público y su tratamiento sea necesario

[228] UNION EUROPEA. 1995. Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Octubre 1995.
[229] ESPAÑA. 1999. Ley Orgánica 15/99, de Protección de Datos de Carácter Personal. Diciembre 1999.

para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado". Cabe hacer presente que al momento de la discusión parlamentaria de la ley chilena de protección de datos, la ley que regulaba el tratamiento de datos personales en España era la LORTAD[230], que al igual que su sucesora la LOPD, reconocía la existencia de las fuentes accesibles al público, pero de una manera mucho más abierta, ya no se les definía respecto a determinadas hipótesis (censo, guías telefónicas, colegios de profesionales) sino que de manera general sólo se limitaba a señalar que se permitía el tratamiento de datos provenientes de fuentes accesibles al público sin el consentimiento del afectado[231]. Luego el Real Decreto 1332/1994[232], definió a los datos accesibles al público, como "los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo". De su parte, la ley italiana[233] sobre protección de datos, también excepciona a la regla general del consentimiento, cuando los datos provienen de registros públicos, listados, acciones o documentos accesibles por cualquier persona[234]. La ley alemana de protección de datos[235], se refiere en más de una oportunidad al concepto de fuente accesible al público, pero aplicado a determinados ámbitos, y no como una excepción amplia al consentimiento, así, por ejemplo, la sección 29, permite en el caso de agencias de créditos tratar los datos si éstos han sido extraídos de fuentes accesibles al público, a

[230] ESPAÑA. 1992. Ley Orgánica 5/92, de Regulación del Tratamiento Automatizado de Datos. Octubre de 1992.
[231] Artículo 6 LORTAD. Consentimiento del afectado. 1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos.
[232] ESPAÑA. 1994. Real Decreto 1332/94, sobre reglamentación de la LORTAD. Junio 1994.
[233] ITALIA. 1996. Legge N° 675, tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Diciembre 1996.
[234] Artícolo 12 Legge N° 675. Casi di esclusione del consenso. 1. Il consenso non è richiesto quando il trattamento: c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.
[235] ALEMANIA. 2002. Bundesdatenschutzgesetz (BDSG). Enero 2002.

menos que el titular de éstos tenga un interés superior legítimo en orden a no permitir el señalado tratamiento. Por último, en el marco europeo, la ley de protección de datos de Inglaterra[236], también establece una excepción referida a fuentes accesibles al público, pero no, al igual que la ley alemana, como una excepción al consentimiento, sino que como excepción a ciertos principios establecidos en la ley[237]. En el ámbito latinoamericano, las pocas legislaciones que contemplan leyes generales de protección de datos, dentro de las cuales encontramos la argentina y la uruguaya, establecen la excepción de fuentes accesibles al público, así, la ley argentina de protección de datos[238] establece en su artículo 5 número 2 letra a) que no se requiere el consentimiento del titular de los datos cuando los datos se obtengan de fuentes de acceso público irrestricto, no señalando, sin embargo, qué se debe entender por el referido concepto, una norma similar, se contempla en la ley de protección de datos de Uruguay[239], la que indica en su artículo 4° que: "No requiere previo consentimiento el registro y posterior tratamiento de datos personales cuando: a) Los datos provengan de fuentes públicas de información, tales como registros, archivos o publicaciones en medios masivos de comunicación".

De lo señalado a propósito del tratamiento de esta excepción en el derecho comparado, se puede concluir que éste es disímil, en algunos países como España y Alemania, se presenta como un concepto restringido, ya sea por su propia definición como en el caso español, ya sea, porque el titular de los datos pueden oponerse a la aplicación de la excepción fundado en un interés superior legítimo. De otra parte, países como Argentina, Uruguay e Italia, incluyen la excepción en forma amplia y sin restricciones.

En el caso chileno, se observa una mezcla de ambas tendencias, ya que si bien se establecen tres hipótesis en que opera la excepción, haciéndola restrictiva, tanto la naturaleza de

[236] INGLATERRA. 1998. Data Protection Act. Octubre. 1998.
[237] Part IV. Exemtions. 34. Personal data are exempt from (a) the subject information provisions, (b) the fourth data protection principle and section 14(1) to (3), and (c) the non-disclosure provisions, if the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.
[238] ARGENTINA. 2000. Ley 25.326 de Protección de los datos personales. Octubre 2000.
[239] URUGUAY. 2004. Ley 17.838 de Protección de datos personales para ser utilizados en informes comerciales y acción de hábeas data. Septiembre 1994.

ellas como la definición legal de fuentes accesibles al público, hacen que en la práctica, la excepción sea utilizada con gran amplitud[240].

2.6.1.2. Historia de la ley

Esta excepción no estaba contemplada en el proyecto de ley original, recién se incorporó en el segundo informe de la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados, con una redacción que incluía dos de las hipótesis que existen en la Ley vigente, a saber: la referida a los datos patrimoniales y a los datos contenidos en listados relativos a una categoría de personas[241].

Ya en el tercer trámite constitucional la Comisión de Constitución, Legislación y Justicia de la Cámara del Senado estimó conveniente acoger una sugerencia formulada por los Ministerios Secretaría General de la Presidencia y de Justicia, en el sentido de intercalar una letra nueva, en la que se defina el concepto de fuentes accesibles al público," lo que permitiría hacer claridad en cuanto al alcance de dicha expresión, que tiene particular relevancia para determinar los casos de excepción en que no se requiere autorización del titular de los datos personales para someterlos a tratamiento"[242].

La letra nueva que se propuso por la Comisión fue: "h) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes." Definición que fue aprobada, y forma parte actualmente del artículo 2 de la Ley.

[240] Prueba de ello, es la gran cantidad de sentencias, que se apoyan en la excepción "fuentes accesibles al público", para rechazar recursos de protección interpuestos en contra de empresas que efectúan tratamiento de datos patrimoniales. Ver: sentencias de Corte de Apelaciones de Santiago, rol 4934-2000 de 26.11.2002; rol 4915-2000 de 21.12.2000; rol 4371-2001 de 30.01.2001; rol 4013-2000 de 11.12.2000; rol 246-2000 de 27.07.2000; rol 1797-2000 de 25.05.2000 y rol 1396-2000 de 30.05.2000, sentencias de Corte de Apelaciones de Concepción, rol 3395-2000 de 26.03.2002, rol 2381-2001 de 21.09.2201, rol 2346-2001 de 07.11.2001.

[241] El artículo 5 inciso 5 en comento indicaba: "No requiere autorización la recolección o comunicación de datos personales de carácter económico, financiero, bancario o comercial que provengan o se recojan de fuentes accesibles al público, o de datos personales contenidos en listados relativos a una categoría de personas, en la medida que se limiten a indicar la pertenencia del individuo a ese grupo, a señalar su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento."

[242] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2094. 05 de agosto de 1993.

Por último, la Comisión, coincidió en la necesidad de aclarar que estas tres únicas excepciones[243] sólo pueden referirse a datos personales que provengan o que se recolecten de fuentes accesibles al público[244].

Luego, la Comisión Mixta en su informe, efectúa ciertas aclaraciones de importancia al momento de interpretar la excepción de fuentes accesibles al publico, indica que: "las excepciones a la exigencia de autorización se entienden siempre referidas a datos personales que provengan o que se recolecten de fuentes accesibles al público. Dentro de ese marco general, se enuncian de manera taxativa tres situaciones en que deben encontrarse los datos: ser de carácter económico, financiero, bancario o comercial; estar contenidos 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 ser necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios" y que "El concepto de "fuentes accesibles al público" que se usa en el inciso quinto, y que está definido en el artículo 2º, letra h), se refiere a registros de datos personales que están conformes a derecho, no a aquellos de carácter ilegal. Por ende, la mención de este inciso a datos personales provenientes o recolectados de tales fuentes alude a datos obtenidos lícitamente"[245].

De la historia de ley se puede concluir que las hipótesis a las cuales se les aplica la excepción de fuente accesible al público son taxativas y alternativas y que debe tratarse de fuentes que contengan datos obtenidos legítimamente, esto es, en cumplimiento de la legislación y especialmente, de las normas establecidas en la Ley 19.628.

---

[243] Esto es: a) Cuando sean datos de carácter económico, financiero, bancario o comercial, o; b) Cuando sean datos que 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; c) Cuando sean datos necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.
[244] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2103. 05 de agosto de 1998.
[245] Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 106. 02 de junio de 1999.

2.6.1.3. Alcance del concepto fuentes accesibles al público

Del estudio de la historia de la ley no se puede colegir cuál es el verdadero sentido y alcance del concepto fuentes accesibles al público, el cual como ya hemos señalado, resulta esencial para determinar la amplitud de la excepción. Al respecto la escasa doctrina nacional, esboza dos soluciones: o se entiende que todas las fuentes de datos personales serán de acceso público, no restringido o reservado a los solicitantes, salvo que una ley establezca lo contrario, es decir, que una ley señale que determinado registro o fuente es reservada, o bien, se entiende que todas las fuentes de datos personales son de acceso restringido salvo que una ley señale lo contrario, es decir, que una ley señale que determinado registro o fuente es público.

Basado en tres argumentos Alberto Cerda indica que la segunda interpretación es la correcta, sus argumentos son los siguientes: "primero, la ley en examen ha pretendido brindar protección a la vida privada y tal espíritu se aviene mejor con ella; segundo, la información recogida de fuente accesible al público hace excepción a la regla general, cual es que el procesamiento de datos personales supone el consentimiento informado del titular de ellos, en consecuencia debe ser interpretada en un sentido restrictivo; y, tercero, aún cuando existen disposiciones legales que prevén la confidencialidad o secreto de ciertos datos, su propósito no ha sido, siquiera lejanamente, adjudicar publicidad a situaciones diversas de las por ellas regladas"[246].

Renato Jijena, de su parte, sostiene la tesis contraria, fundamentalmente debido a que, según indica, 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 reservados o confidenciales, por ejemplo, el secreto bancario o el secreto de filiación política, de manera que al existir tales normas, son de acceso restringido; si no existieran (que es la regla general) serán de acceso permitido o fuentes públicas, así concluye que en Chile todas las fuentes de datos personales serán en principio y por regla general y legalmente de acceso público, no restringido o reservado a los solicitantes, salvo, que una ley especial -como las

[246] CERDA, Alberto. op. cit. pág. 70.

nombradas-, o una norma o resolución administrativa o una cláusula contractual de confidencialidad, establezcan expresamente lo contrario[247].

Por nuestra parte, compartimos en parte este último criterio, en primer lugar, porque cuando la ley ha querido darle el carácter secreto y/o confidencial a una determinada información, así lo ha hecho en forma expresa, como por ejemplo, respecto a los secretos estadísticos, bancarios, tributarios o de filiación política. Lo anterior, sobre todo teniendo presente que en nuestro ordenamiento en el ámbito público, rige como regla general la publicidad y el secreto opera sólo como excepción[248]. De manera que, a lo menos, en el ámbito público es que las fuentes de datos personales sean públicas, salvo una norma establezca lo contrario.

Sin embargo, la conclusión anterior no es tan clara en el ámbito privado, ¿podemos concluir aplicando lo señalado anteriormente que todas los registros de datos personales de naturaleza privada constituyen, por regla general, fuentes accesibles al público, ya que su acceso es irrestricto o permitido a quien lo solicite? La conclusión que se obtenga no es baladí, y creemos que se debe solucionar caso a caso, convirtiéndose en una cuestión de hecho que deberá en su momento ser interpretada por los Tribunales de Justicia[249].

De esta manera, y a modo de conclusión, para poder determinar si estamos en presencia de una fuente accesible al público o no, debemos establecer en primer lugar, su naturaleza, así, si

[247] JIJENA, Renato. La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos. 2001. En: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 85-111.

[248] La Ley 19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado, indica en su artículo 16: "Principio de Transparencia y publicidad. El procedimiento administrativo se realizará con transparencia de manera que permita y promueva el conocimiento, contenidos y fundamentos de las decisiones que se adopten en él.
En consecuencia, salvo las excepciones contenidas en la ley en el reglamento, son públicos los actos administrativos de los órganos de la Administración del Estado, y los documentos que le sirvan de sustento o complemento directo o esencial". CHILE. Ley 19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado. Mayo 2003.

[249] Así por ejemplo, en el caso de los datos patrimoniales que poseen el Boletín Comercial o DICOM, es claro, que se trata de fuentes accesibles al público, ya que cualquiera puede acceder a ellos pagando determinada cantidad de dinero en forma previa; no existe acá un acceso restringido a los solicitantes. Pensemos ahora, en los mismos tipos de datos patrimoniales, pero que son tratados en esta ocasión por una casa comercial, en este caso, usted no obtendrá un resultado positivo si se acerca a la casa comercial solicitando acceder a los datos de una persona distinta de usted, de manera que en este tipo de casos, se trata de fuentes que a la luz de la definición legal no son accesibles al público.

se trata de un banco de datos público, esto es, cuyo responsable del tratamiento es un órgano público, se tendrá que indagar si existe alguna norma que establezca el carácter de secreto o de acceso restringido a los solicitantes respecto del tipo de dato específico que se solicita, lo anterior porque en el ámbito público rige como regla general el principio de la publicidad, constituyendo la excepción el secreto o reserva, así por ejemplo, si se visita la página web del Servicio de Registro Civil e Identificaciones[250], se podrá observar que se ofrece el servicio de venta de certificados de nacimiento, defunción, matrimonio, anotaciones vigentes de vehículos motorizados en forma no restringida a quien los solicite, sin embargo, no se permite acceder en forma irrestricta, y por lo tanto no se vende el servicio, a certificados que digan relación, por ejemplo, con el historial penal de una determinada persona, ya que en este caso, sí existe una norma legal que establece su secreto[251]. En el ámbito de las fuentes de datos personales privadas, ya no podemos aplicar el referido principio de publicidad que sólo es propio del ámbito público, por lo que se deberá analizarse el caso concreto, distinguiendo si el responsable del banco de datos respectivo permite el acceso a los datos personales a quien los solicite, o en otras palabras, en forma no restringida[252], en cuyo caso, estamos en presencia de una hipótesis de fuente accesible al público, o bien, si el responsable del banco de datos respectivo no entrega los datos a quien lo solicite o lo hace sólo a su titular, caso en el cual, claramente no nos encontramos ante una fuente accesible al público.

Finalmente, la existencia del concepto de fuentes accesibles al público en la Ley 19.628, no sólo produce la ausencia de consentimiento del titular para el tratamiento de sus datos personales en las tres hipótesis revisadas, sino que además implica que ciertas obligaciones establecidas en la ley como regla general, también sufran una excepción, así:

a) La obligación de secreto sobre los datos personales, como asimismo, sobre los demás datos y antecedentes relacionados con el banco de datos, que se establece en el artículo 7

[250] SERVICIO DE REGISTRO CIVIL E IDENTIFICACIONES [en línea] <http://www.registrocivil.cl/ofinternet/doAction?actionName=viewMenuCertificados&modoEnvio=onLine> [consulta: 12 enero 2004].

[251] CHILE. 1925. Decreto Ley N° 645 sobre el Registro Nacional de Condenas. Octubre 1925. Cuyo artículo 6 indica "Fuera de las autoridades judiciales, policiales y de Gendarmería de Chile respecto de las personas sometidas a su guarda y control, nadie tiene derecho a solicitar la exhibición de los datos que se anotan en el Registro"

[252] Desde nuestro punto de vista, el cobro de una tarifa por el acceso a una determinada base de datos es indiferente a efectos de calificar a una determinada fuente como de acceso público, lo

de la ley y que pesa sobre las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados no aplica cuando tales datos provengan o hayan sido recolectados de fuentes accesibles al público[253].

b) El importante principio de finalidad que exige que los datos personales deben utilizarse sólo para los fines para los cuales han sido recolectados no aplica, conforme el artículo 9 de la ley, a los datos que provengan o se hayan recolectado de fuentes accesibles al público[254].

c) Por último, tampoco se aplican los requisitos que establece el artículo 5 de la ley, para los procedimientos automáticos de transmisión de datos personales y requerimientos de datos personales mediante una red electrónica, cuando los datos personales sean accesibles al público en general, es decir, conforme a la definición legal, cuando se trate de fuentes accesibles al público[255].

2.6.1.4. Hipótesis de aplicación excepción fuentes accesibles al público

En último lugar, efectuaremos respecto a cada uno de los tipos de datos provenientes de fuentes accesibles al público de que trata esta excepción, algunos comentarios destinados a aclarar su ámbito de aplicación.

---

determinante es que en los hechos efectivamente cualquiera que lo solicite, pueda acceder a ella, ya sea en forma gratuita o mediante el pago de un determinado precio o tarifa.

[253] Art 7 Ley 19.628: "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 el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo".

[254] Art 9 Ley 19.628: "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".

[255] Art. 5 Ley 19.628: "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".

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

Respecto a esta excepción, cabe preguntarse si se trata acá del mismo tipo de datos que regula la Ley en su Título III "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", que se refiere sólo a aquellos datos patrimoniales negativos, esto es, a aquellos que dan cuenta de la existencia de alguna obligación o deuda y se encuentran específicamente establecidos en el artículo 17, o bien, se trata de cualquier tipo de dato de naturaleza patrimonial. La distinción es de importancia, tanto desde un punto de vista teórico como práctico, ya que si entendemos que la excepción se refiere sólo a los datos patrimoniales regulados en el Título III de la ley, no estará permitido tratar sin autorización del titular datos, datos patrimoniales positivos, como por ejemplo, el nivel de ingresos de una persona, sus propiedades, etc. Lamentablemente la jurisprudencia no ayuda a aclarar esta duda, ya que a hasta el momento no se ha pronunciado respecto a este punto. De su parte, Renato Jijena[256] se inclina, aun cuando no en forma expresa, por señalar que esta excepción abarcaría ambos tipos de datos patrimoniales, es decir, negativos (los del Título III) y positivos, el resto. Existen argumentos para fundamentar la dos interpretaciones posibles: La excepción se refiere sólo a los datos regulados en el Título III, ya que aun cuando la ley no distingue, se debiera entender así, dado el espíritu de la legislación, a lo menos el declarado, cual es brindar protección a los titulares de datos personales y porque tanto la excepción de que se trata como el Título III de la ley se incluyeron en la misma etapa de tramitación legislativa, lo que llevaría a concluir que los legisladores estaban pensando en la misma hipótesis de datos[257]; asimismo, podemos fundamentar que la excepción abarca todo tipo de dato patrimonial, dado que el legislador no distingue, no pudiendo, en consecuencia, el intérprete distinguir y porque el Título III habla de obligaciones de carácter económico, financiero, bancario o comercial y la excepción se refiere a datos de carácter económico, financiero, bancario o comercial (sin mencionar que se trate de obligaciones), y por último, porque así lo pareció entender uno de los Senadores que participó activamente en la tramitación del proyecto de ley respectivo[258].

[256] JIJENA, Renato. op. cit. pág. 99.
[257] Tanto la excepción en estudio como el actual Título III de la Ley 19.628, fueron incorporados al proyecto de ley respectivo, por la Cámara de Diputados en el mismo momento; en el Segundo Informe de la Comisión de Constitución, Legislación y Justicia.
[258] De la intervención del Senador Viera-Gallo, se puede colegir que entiende que en la excepción se comprenderían todos los datos patrimoniales y no sólo los negativos. "En el caso de los privados, en especial de las empresas que se dedican estas actividades, se requiere de autorización expresa del afectado, la cual debe darse por escrito. Es decir, un tercero no puede recolectar, almacenar,

Creemos que frente a estas dos posibles interpretaciones, la segunda es la correcta, tanto por la historia de la ley como por el tenor literal de la norma que no distingue entre datos patrimoniales negativos o positivos.

b) Cuando sean datos que 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.

Esta hipótesis, parece tener su fuente en el Real Decreto 1332/94 reglamentario de la LORTAD española, que indica dentro de las hipótesis de datos accesibles al público, aquellos datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo. Sin embargo, nuevamente la ley chilena, es más amplia, ya que no restringe la hipótesis a los colegios profesionales sino que a los datos que se contengan en listados relativos a una categoría de personas. La enunciación de los datos que debieran contener estos listados relativos a una categoría de personas, tiene claramente un tenor ilustrativo, al utilizarse las palabras "tales como"[259].

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

Esta hipótesis se refiere a la actividad conocida como marketing directo, que constituye una manera de efectuar en forma activa y directa promoción y publicidad de determinados

---

procesar, transmitir ni comercializar datos de las personas si no hay una autorización expresa del afectado. Existen excepciones a este principio: En primer lugar, el proyecto dispone que los datos económicos que provienen de fuentes públicas pueden ser almacenados y procesados sin la autorización de los afectados, porque su origen es una fuente pública Por ejemplo, son datos públicos, los extractos de las sociedades anónimas publicados en el Diario Oficial, los protestos de letras y cheques del boletín de la Cámara de Comercio, el registro de propiedades del Conservador de Bienes Raíces y el extracto de declaración de impuestos. Entonces una empresa privada como DICOM, la más conocida, podrá recolectar, almacenar y procesar datos siempre y cuando provengan de fuentes públicas". Cámara de Diputados. Segundo Trámite. Sesión 13, pág. 23. 05 de noviembre de 1997.

[259] Así se señaló, además, en tercer trámite constitucional de la tramitación del respectivo proyecto de ley en el Informe de la Comisión de Constitución Legislación y Justicia del Senado: "En relación con el caso de los listados relativos a categorías de personas, se precisó también que las menciones que se

productos y/o servicios. Uno de los insumos necesarios para efectuar marketing directo son los bancos de datos personales que dan cuenta de los gustos, preferencias, datos de identidad, entre otros de los destinatarios de las comunicaciones de marketing. A diferencia de los otros dos casos que contempla esta excepción, no encontramos en la legislación extranjera, mención relativa esta hipótesis en tanto excepción a la autorización del titular de los datos, por el contrario, incluso la ley danesa de protección de datos personales[260] prohíbe expresamente a las compañías ceder datos relativos a un cliente a una tercera compañía con propósitos relacionados con el marketing o usar datos en nombre de una tercera compañía para este propósito, salvo que el titular del datos haya dado su consentimiento explícito. Su inclusión en la ley se explica por el *lobby* efectuado por empresas que realizan marketing directo[261], que incluso, solicitaban ampliar más la excepción en estudio, sin embargo, a la Comisión de Constitución, Legislación y Justicia del Senado no le pareció apropiado extender las excepciones a la obligación de autorización previa a más casos de los contemplados en el precepto aprobado por la H. Cámara de Diputados, con la salvedad de la actividad de comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios, que prefirió incluir para evitar dudas, aunque la entendió comprendida en las dos situaciones ya descritas[262].

Cabe señalar asimismo, dos artículos de la ley que dicen relación con el marketing directo y la autorización y revocación del titular de los datos. De una parte, el artículo 12 inciso 3 otorga al titular de los datos respectivo el derecho de exigir al responsable de este tipo de

---

señalan lo están por vía simplemente ilustrativa". Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2103. 05 de agosto de 1993.

[260] DINAMARCA. 2000. Lov N° 429 af 31 maj 2000 som aendret ved lov N° 280 af 25 april 2001. Mayo 2000.

[261] La Asociación de Marketing Directo de Chile A.G. expuso que el "marketing directo" permite a los consumidores recibir información suficiente para tomar decisiones que constituyan una elección educada de productos, servicios, representantes políticos o gremiales, entre otros. Las personas son conectadas a través del correo, en televisión o en cualquier otro medio o, más frecuentemente, porque aparecen en listados que la empresa de "marketing directo" ha escogido, considerando que representan un grupo grande de personas que podrían estar interesadas en la oferta. Se hizo presente que el sistema de protección que contemplaba la norma en tramitación, entraba complica y limita, no sólo la actividad de "marketing directo", que es lícita, sino que el derecho a la información de los potenciales usuarios del mismo, quienes, cada vez que deseen recibir información respecto de un determinado producto o servicio, deberían otorgar su expresa autorización, o bien tendría la empresa de "marketing directo" que cumplir con engorrosos y costosos procedimientos. En esa virtud, planteó la necesidad de darle a las personas el derecho de recibir libremente y sin limitaciones, las informaciones que le permitan elegir más adecuadamente y contemplar el derecho a excluirse, comunicándolo expresamente a la empresa que le envió la información. Diario Sesiones del Senado. Sesión 63, tomo 7383, pág. 7486. 17 de mayo de 1995. Es decir se opta acá por el sistema de autoexclusión u *opt-out*, como quiera llamársele, sistema que en definitiva fue el acogido por la ley de protección de datos chilena en esta materia.

[262] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2103. 05 de agosto de 1998.

bancos de datos personales, ya sea la eliminación o el bloqueo de sus datos personales, ya sea en forma temporal o definitiva, cuando ellos se usen para comunicaciones comerciales y no se desee continuar figurando en el registro respectivo[263]. Así, se ha señalado que en el caso de los datos personales que se usen para comunicaciones comerciales, sea cual fuere la fuente de la autorización, si el titular de los datos no desea continuar figurando en el registro respectivo, puede solicitar la eliminación o bloqueo de sus datos[264]. Asimismo, opera respecto de este tipo de tratamiento el denominado derecho de oposición, que se encuentra consagrado en le artículo 3 de la Ley, cuando indica en su inciso segundo que el titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión[265].

Duramente ha sido criticada esta norma que permite el tratamiento de datos personales sin autorización del titular de los datos respectivos con el objeto de efectuar marketing directo por algunos autores que, incluso han esbozado inconstitucionalidad, como Renato Jijena quien señala: "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"[266]. De su parte, Alberto Cerda señala que esta disposición "ha tenido por propósito legitimar el tratamiento de datos personales efectuados por las empresas de marketing directo, en las cuales se trata información conducente a establecer comunicación entre prestadores de servicios y los

[263] Art. 12 inciso 3 Ley 19.628: "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".

[264] JARA, Rony. 2001. Régimen jurídico de los datos de carácter económico, financiero, bancario o comercial en la Ley N° 19.628. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 61-83.

[265] A este respecto Renato Jijena ha señalado que "el artículo 4 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 la que se refieren) puede oponerse –a 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". JIJENA, Renato. op. cit. pág. 102. No compartimos el criterio señalado; en nuestra interpretación, lo correcto es señalar que puede efectuarse tratamiento de datos, sin autorización del titular, con fines de marketing directo cuando los referidos datos han sido extraídos de fuentes accesibles al público, teniendo en todo caso el titular de los datos derecho a oponerse a la utilización de sus datos con fines de publicidad, derecho de oposición que se hace efectivo en la práctica, mediante el ejercicio del derecho de cancelación o bloqueo que se estatuye en el artículo 12 inciso 4 de la Ley.

[266] JIJENA, Renato. op. cit. pág. 103.

consumidores"[267]. Por último, Pablo Palazzi señala que "Esta es una limitación que no está presente en la Directiva y que hace a la ley chilena una ley demasiado benévola, casi se podría afirmar hecha "a medida" de ciertos sectores, pues las excepciones están redactadas definiendo a actividades por todos conocidas"[268].

2.6.2. Datos personales tratados por personas jurídicas privadas.

Esta segunda categoría de datos personales que se refiere al tratamiento que de ellos efectúan personas jurídicas privadas, tampoco requiere autorización del titular de los datos; la excepción se encuentra establecida en el inciso final del artículo 4 que indica que "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."[269]

En un principio la norma no hacía mención al concepto de personas jurídicas privadas, sino que al de asociaciones gremiales, por cuanto fue la Asociación de Aseguradores de Chile A.G., una asociación gremial, la que instó por la inclusión de esta excepción[270]. Luego, sin

[267] CERDA, Alberto. op. cit. pág. 71.
[268] PALAZZI, Pablo. op.cit. pág. 180.
[269] Una norma parecida fue establecida en la LOPD española en la disposición adicional 6ª, que dispuso: "Se modifica el artículo 24.3, párrafo 2º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados con la siguiente redacción: "Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley. También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación. En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado."
[270] "…la sustitución del inciso final obedeció a la necesidad de abarcar situaciones que de otra manera quedarían injustificadamente excluidas. El debate que condujo a tomar esa determinación se originó con motivo de la situación que hizo presente la Asociación de Aseguradores de Chile A.G., en orden a que ella ha desarrollado dos bases de datos; una relacionada con el pago de pensiones de invalidez y otra relativa al sistema de información de siniestros de seguros generales, las cuales no podrían seguir existiendo si se limitara la información de que puede ser objeto de tratamiento de los datos personales de asociados"… "A la luz de esos antecedentes, la Comisión Mixta resolvió aprobar, como inciso final, una disposición en virtud de la cual no se requerirá autorización para el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, el de sus asociados y el de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos". Diario Sesiones del Senado. Sesión 2, s/tomo, pág. 107. 08 de marzo de 1998.

embargo, la Comisión de Constitución, Legislación y Justicia del Senado[271] concordó en utilizar, en vez de la expresión asociaciones gremiales, que tiene un sentido jurídico determinado, referido a las asociaciones reguladas por el decreto ley N° 2.757, de 1979, una más genérica como es la de "personas jurídicas privadas", y puntualizar que la excepción de la autorización se refiere a aquellos datos personales de sus asociados, siempre que estén destinados al uso exclusivo de la persona jurídica, para fines estadísticos, de tarificación u otros de beneficio general de los mismos asociados.

Cabe llamar la atención respecto a la imposibilidad de comunicar los datos por parte de las personas jurídicas privadas que efectúen tratamiento a partir de esta hipótesis, ya que la norma en comento, sólo las autoriza a efectuar tal tratamiento para su uso exclusivo, lo que implica que no pueden comunicar esos datos a terceros, ya que en este supuesto, serían estas terceras partes las que estarían utilizando los datos personales y no en forma exclusiva las personas jurídicas privadas.

2.6.3. Datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial.

2.6.3.1. Nociones Previas

La Ley 19.628 reconoce otra categoría de datos, que llamaremos datos patrimoniales negativos comunicables[272], dedicando un título especial a ellos: el Título III denominado “De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial”, compuesto de tres artículos. Respecto a esta categoría de datos personales, tampoco se requiere la autorización del titular de ellos para efectuar su tratamiento si los datos se recogen de fuentes accesibles al público, por aplicación de lo señalado en el artículo 4 de la ley, sin embargo, la comunicación que de ellos se puede efectuar, ya sea se extraigan de

[271] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2103. 05 de agosto de 1998.
[272] En el ámbito de los datos personales patrimoniales, se suele distinguir entre aquellos que son de naturaleza negativa, y los que lo son de índole positiva. Así, serán datos patrimoniales negativos, aquellos que den cuenta de obligaciones o deudas que tenga una determinada persona, en términos contables: su pasivo. Por el contrario, los datos patrimoniales positivos, son aquellos que se refieren a aquella parte del activo del patrimonio de una persona (bienes, dinero, propiedades, etc.). Esta distinción es de suma importancia, ya que como veremos, el tratamiento legislativo y también

fuentes accesibles al público o no, se encuentra permitida sin la autorización del titular de los datos y a la vez restringida por las normas que se establecen en el Título III de la Ley al que hacemos referencia[273]. De esta manera, se produce el siguiente fenómeno: Se pueden tratar de datos patrimoniales negativos si este tratamiento ha sido autorizado por el titular (autorización convencional) o por la ley a través de la excepción de fuente accesible al público (autorización legal), sin embargo, algunos de estos datos (los que se encuentren fuera del listado que se contempla en el artículo 17), no pueden ser comunicados, pero sí tratados[274]. En cambio, si estamos en presencia de datos patrimoniales positivos, éstos siempre serán tratables sin autorización del titular si se han extraído de una fuente accesible al público, en caso contrario requerirán de autorización del titular de los datos o de otra ley.

2.6.3.2. Derecho Comparado

En el ámbito del derecho comparado, encontramos varias legislaciones que le otorgan un estatuto o tratamiento especial a los datos patrimoniales o también denominados de solvencia económica o crediticia, tal como lo efectúa la ley chilena. La LOPD española, dedica un artículo especial a este tipo de datos[275], regulándolos de forma más amplia que la ley chilena, pues la LOPD no sólo norma la comunicación de estos datos, como es en el caso chileno, sino que en

doctrinario que se efectúa respecto a los datos patrimoniales es totalmente distinto en uno y otro caso.

[273] Fuertemente ha sido criticada por Rony Jara la creación por el legislador de esta categoría especial de datos, esgrimiendo que "estos datos tienen el carácter de supraindividuales y que por lo tanto, aunque se estime que ellos pudieran formar parte de la intimidad de la persona, por su propia naturaleza y rol en la sociedad, el derecho a su conocimiento por terceros se impone por sobre la protección a la intimidad...pudieron armonizarse en mejor forma los derechos del titular y los terceros, mediante el recurso a ciertos procesos de seriedad *ex ante* o de responsabilidades *ex post"*. JARA, Rony. op. cit. pág. 74.

[274] Es decir, existe una categoría de datos patrimoniales negativos que no son comunicables, pero si tratables. Ver en el mismo sentido JARA, Rony. Ibíd.

[275] Artículo 29 LOPD. Prestación de servicios de información sobre solvencia patrimonial y crédito. 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley. 3. En los supuestos a que se refieren los dos apartados anteriores cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos. 4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran,

forma general regula el tratamiento de datos que efectúan los prestadores de servicios de información sobre solvencia patrimonial y crédito. Una de las características interesantes de la legislación española, es que establece expresamente las fuentes de las cuales se puede extraer este tipo de datos, así indica que ellos podrán ser obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento (se refiere acá a datos patrimoniales positivos), indicando que podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés (se refiere acá a datos patrimoniales negativos)[276].

En el ámbito latinoamericano, la ley argentina de protección de datos personales[277] posee una norma muy parecida a la española, por lo que en esta parte, nos remitimos a los comentarios efectuados respecto de esta última. La ley uruguaya de protección de datos[278], que tiene por objeto regular en forma específica los datos de naturaleza patrimonial, efectúa un tratamiento más amplio que la ley chilena, ya que no restringe la regulación sólo a la comunicación, sino que al tratamiento de los señalados datos en general, indicando en su artículo 8 que "Queda

---

cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos.

[276] "Por tanto, en estos ficheros son posibles dos categorías diferentes de datos personales, tal y como ya sucedía en la LORTAD: a) Por una parte, datos relativos a la solvencia patrimonial y el crédito de naturaleza positiva, entendida como información sobre las posibilidades económicas y financieras de una persona física y, b) por otra parte, datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias. Respecto a la primera categoría de datos personales, las fuentes de obtención de información podrán ser: fuentes accesibles al público, datos facilitados por el propio afectado e información obtenida de cesiones consentidas por el propio interesado. Respecto a la segunda categoría de datos personales, las fuentes de obtención de información, se restringen a dos: el propio acreedor, y quien actúe por su cuenta o interés. Ya que es fácil imaginar que nadie se acusará a sí mismo de no estar al corriente en el pago de sus de sus deudas, por lo que dicha información la reservará para sí." HERRÁN, Ana. op.cit. pág. 299.

[277] Art. 26.- Prestación de servicios de información crediticia. 1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés. 3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión. 4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho. 5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

[278] URUGUAY. 2004. Ley 17.838 de Protección de datos personales para ser utilizados en informes comerciales y acción de hábeas data. Septiembre 1994.

expresamente autorizado el tratamiento de datos personales relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias del artículo 4"[279], como se puede observar la ley uruguaya también presenta mayor amplitud que las otras legislaciones revisadas y también que la chilena, en cuanto, se permite el tratamiento de datos patrimoniales sin autorización del titular en casos que no se encuentran contemplados en las referidas legislaciones.

2.6.3.3. Historia de la ley

Ya analizando el caso chileno y como se aprecia de la historia de la ley[280], la Comisión Mixta debatió ampliamente en su seno la extensión que debía dársele a este Título III, es decir, qué tipo de obligaciones de carácter comercial, económico, bancario y financiero podrían ser incluidas en un banco de datos[281], y por ende, ser comunicadas. Una posibilidad era entender ese concepto en forma amplia, de modo que los bancos de datos pudieran tratar datos personales que dieran cuenta de diferentes tipos de incumplimientos de obligaciones pecuniarias, como aquellas referidas a cuentas por consumo de servicios, contratos de arriendo, facturas, colegiaturas y cualesquiera otras. Tal criterio se sustentaría en la necesidad de considerar, para el adecuado funcionamiento de la actividad económica, la mayor cantidad de información posible acerca del comportamiento económico de las personas, que en algún momento pudiera ser de interés para

[279] El señalado artículo 4° de la ley de protección de datos uruguaya indica que: "No requiere previo consentimiento el registro y posterior tratamiento de datos personales cuando: A) Los datos provengan de fuentes públicas de información, tales como registros, archivos o publicaciones en medios masivos de comunicación; B) Sean recabados para el ejercicio de funciones o cometidos constitucional y legalmente regulados propios de las instituciones del Estado o en virtud de una obligación específica legal; C) Se trate de listados cuyos datos se limiten a nombres y apellidos, documento de identidad o registro único de contribuyente, nacionalidad, estado civil, nombre del cónyuge, régimen patrimonial del matrimonio, fecha de nacimiento, domicilio y teléfono, ocupación o profesión y domicilio; D) Deriven de una relación contractual del titular de los datos y sean necesarios para su desarrollo y cumplimiento; y E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo o el de sus asociados o usuarios.

[280] Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 122. 02 de junio de 1999.

[281] Se observa la confusión existente en la Comisión Mixta, en lo que respecta a esta parte de la discusión parlamentaria del proyecto de ley, a propósito de los conceptos de almacenamiento, tratamiento y comunicación de datos personales. En definitiva, y en estricto sentido, el Título III de la ley no reguló los datos que podían "ser incluidos" en un banco de datos, sino los que pueden ser comunicados. Existe una relación de género a especie entre el tratamiento de datos y la comunicación de datos, así toda comunicación de datos implica un tratamiento de ellos, pero no todo tratamiento de datos implica una comunicación de ellos.

terceros conocerla. La otra opción analizada por la Comisión Mixta fue la de precisar de un modo taxativo las obligaciones impagas de carácter económico, financiero, bancario y comercial que podrían ser tratadas[282] en un banco de datos personales, con exclusión de cualquiera otra. Esta opinión se fundaría en que, si bien existe una conveniencia social de conocer parte de esta información, hay siempre otra parte que la persona tiene derecho a conservar en reserva, por múltiples razones, como afectar un ámbito más íntimo, su menor trascendencia, su dudoso fundamento o exigibilidad, etc., y porque era el criterio normativo vigente en la materia, que se refleja en la reglamentación del Boletín de Informaciones Comerciales. Finalmente, la Comisión Mixta por la unanimidad de sus integrantes, se manifestó partidaria de seguir ese criterio, en orden a circunscribir el tratamiento (en realidad, la comunicación) de datos personales de carácter económico, financiero, bancario y comercial a los actuales incumplimientos de obligaciones que se publican en el Boletín de Informaciones Comerciales[283] que se encuentra regulado en el Decreto Supremo de Hacienda N° 950 de 1928[284].

2.6.3.4. Tipos de datos patrimoniales negativos comunicables

De esta manera, se aprobó como artículo 17 una disposición en virtud de la cual 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, que se encuentren en cualquiera de las siguientes tres hipótesis:

i) cuando consten en letras de cambio y pagarés protestados;

ii) cuando consten en cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa, y

iii) cuando se trate del incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de

[282] Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 123. 02 de junio de 1999.

[283] Agregándose la posibilidad de comunicar el incumplimiento de obligaciones con sociedades administradoras de créditos otorgados por compras en casas comerciales, a sugerencia de la Cámara de Comercio de Santiago y a criterio de la Comisión Mixta, la posibilidad de comunicar 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. Ibídem.

[284] La ley 19.628 incluyó un artículo 3° transitorio que indica que: "Las normas que regulan el Boletín de Informaciones Comerciales creado por Decreto Supremo de Hacienda N° 950 de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley." De manera que, el Decreto Supremo de Hacienda N° 950 de 1928 se mantiene vigente, pero en caso de contradicción o

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.

Asimismo, se establece que 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[285]. Lo anterior, se incluyó, ya que "Con ello se otorga la necesaria flexibilidad al sistema, pero estableciendo parámetros mínimos que deberá considerar el Ejecutivo, sin perjuicio de la evaluación caso por caso que le corresponderá efectuar"[286].

El citado artículo 17 fue reformado en el año 2002, a través de la denominada Ley Dicom[287], única que ha modificado la Ley 19.628, prohibiendo la comunicación de los siguientes datos:

---

conflicto entre las normas que regulan los datos patrimoniales negativos establecidas en el referido Decreto Supremo y las normas de la Ley 19.628, primarán estas últimas.

[285] La inclusión en la ley de esta facultad ha sido criticada por varios autores tanto nacionales, como extranjeros, tachándola de ser una norma inconstitucional y de fuente de posibles vulneraciones al derecho a la privacidad. Ver PALAZZI, Pablo. op. cit. pág. 176, quien indica que esta delegación al Presidente para que incluya nuevas excepciones, atentará, en definitiva, contra la integridad del sistema de protección de datos de la privacidad en Chile. En el ámbito nacional, Raúl Bertelsen indica a propósito de esta facultad del Presidente, que "Cabe dejar constancia de la controvertible constitucionalidad de la norma del inciso segundo del artículo 17 de la ley, que confiere competencia al Presidente de la República para autorizar la comunicación de otras obligaciones de dinero, distintas a aquellas mencionadas en el inciso primero del artículo. Lo anterior, teniendo presente que, la intervención en un ámbito privado como el de los documentos que dan cuenta de dichas obligaciones sólo puede ser ordenado por ley para casos determinados con precisión." BERTELSEN, Raúl. op.cit. pág. 118.

[286] Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 125. 02 de junio de 1999.

[287] CHILE. 2002. Ley N° 19.812 modifica la Ley 19.628 sobre Protección de la Vida Privada. Junio 2002. La ley tuvo su origen en una moción presentada por un grupo de diputados, la cual tenía por objeto inicial acortar los plazos establecidos en el artículo 18 de la ley 19.628 para comunicar datos personales negativos a terceros, como una medida para facilitar la reinserción laboral de las personas, ya que con la disminución del referido plazo se limitan los efectos negativos que tiene sobre una gran cantidad de chilenos, el hecho de contar con antecedentes de incumplimientos comerciales, pese a que estas personas han pagado sus deudas o éstas se hayan extinguido por otras causas legales. Moción de los diputados señores Tuma, Elgueta, Bartolucci, Encina, René Manuel García, Montes, Ortiz, Aníbal Pérez, Rocha y la diputada señora Adriana Muñoz que modifica la que modifica la ley 19.628, sobre protección a la vida privada, para favorecer la reinserción laboral de las personas desempleadas. Boletín N° 2735-05. Cabe señalar acá, que la ley en comento, modificó además el artículo 2° del Código del Trabajo, agregando un nuevo inciso 6° que tuvo por objeto evitar las discriminaciones arbitrarias basadas en informes comerciales negativos, del siguiente tenor: "Ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno. Exceptúanse solamente los trabajadores que tengan poder para representar al empleador, tales como gerentes, subgerentes, agentes o apoderados, siempre que, en todos estos casos, estén dotados, a lo

i) Relacionados con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario[288].

ii) Relacionados con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas[289].

2.6.3.5. Derecho al olvido

El denominado doctrinariamente como derecho al olvido[290], se encuentra reconocido ampliamente en derecho comparado para los datos patrimoniales negativos, estableciéndose distintos plazos y cómputos respecto de él en las legislaciones protectoras de datos personales.

---

menos, de facultades generales de administración; y los trabajadores que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza.".

[288] Esta modificación fue introducida por indicación de los senadores Moreno y Sabag debido a que "el Instituto de Desarrollo Agropecuario tiene un conocimiento acabado de la situación de cada una de las personas que le han solicitado crédito y, por lo tanto, no requiere mayor información de parte de los bancos de datos personales. Pero, a su vez, envía información para ser comunicada por medio de estos bancos de datos, circunstancia que agrava la situación de esas personas al impedirles adquirir insumos y otros productos, afectando, precisamente, las posibilidades de pago de dichos préstamos. Sostuvo que la gran cantidad de personas involucradas, en su gran mayoría pequeños agricultores, justifica que el pago de los créditos se persiga sólo con los medios normales, sin apremiarlos al mismo tiempo con la comunicación al público de sus deudas, lo que los priva, en la práctica, de realizar cualquier actividad de orden económico como consecuencia de figurar en tales registros. Añadió que INDAP tiene un buen índice de recuperación de créditos, con cifras superiores al 60%, que no se vería perjudicado con la prohibición que plantea." Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, recaído en el proyecto de ley que modifica la ley 19.628, sobre protección a la vida privada, para favorecer la reinserción laboral de las personas desempleadas. Boletín N° 2735-05. p. 4.

[289] Esta modificación fue introducida por indicación de los senadores Moreno y Sabag. Respecto a la indicación aprobada por la Comisión, ésta indico que: "las obligaciones derivadas de la prestación de servicios básicos no están consideradas en el inciso primero del artículo 17, porque no constan en los documentos a que se refiere la parte inicial de esa norma ni son algunos de los préstamos o créditos previstos en la última parte de ella. Esto es, no pueden ser comunicadas si no lo permite expresamente el Presidente de la República, en ejercicio de la atribución que se le confiere en el inciso segundo del mismo precepto. No obstante lo anterior, en el hecho habría bancos de datos personales que están comunicando algunas de ellas. Frente a esta situación, la Comisión decidió impedir que se comuniquen, prohibiéndolo en forma expresa en el referido inciso segundo del artículo 17. Para evitar dudas de interpretación, precisó que se trata de información relacionada con las deudas que se originen por la prestación de los servicios de electricidad, agua, gas y teléfono." Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, recaído en el proyecto de ley que modifica la ley 19.628, sobre protección a la vida privada, para favorecer la reinserción laboral de las personas desempleadas. Boletín N° 2735-05. p. 4.

[290] La existencia del derecho al olvido se justifica por la doctrina fundamentalmente por razones de índole económica y de garantía al derecho a la privacidad. Así, respecto a este último fundamento HERRAN, Ana. op. cit. pág. 302. señala que: "Constituye un acierto el establecimiento de límites temporales a la conservación de los datos, porque de otro modo no se respetaría para el interesado el derecho al olvido, tan importante en este ámbito donde no sólo se trata de la intimidad de la persona, sino de su honor, y lo que en ocasiones es más perjudicial de la igualdad de oportunidades en el ejercicio de sus derechos, que pueden verse afectados como consecuencia de mantener informaciones inexactas y negativas sobre su persona. Con un fundamento económico JARA, Rony. op. cit. pág 64 indica que "Por otra parte, es necesario considerar que una ley que favorezca la limpieza de antecedentes comerciales, después de transcurrido un cierto plazo, si bien favorece directamente al

Nuestro legislador, también incluyó el derecho al olvido respecto a los datos patrimoniales negativos comunicables, así actualmente, y luego de la reforma introducida por la Ley 19.812, estos datos no podrán ser comunicados después de cinco años desde que la respectiva obligación se hizo exigible o una vez que dicha obligación haya sido pagada o se haya extinguido por otro modo legal (transacción, declaración de nulidad, prescripción, confusión, compensación, etc.)[291]. Con todo, se establece que se comunicará a los Tribunales de Justicia la información que requieran con motivos de juicios pendientes, es decir, que respecto a información requerida por tribunales no rige el derecho al olvido.

Resulta necesario puntualizar que la aplicación del derecho al olvido en Chile, dada la estructura que adopta la regulación del tratamiento de datos personales negativos en nuestra ley, que los regula sólo a propósito de su comunicación en el Título III, no exige que estos datos deban ser eliminados de los bancos de datos, sino que sólo no comunicados, de manera que es perfectamente legítimo tener almacenados y seguir tratando este tipo de datos luego de cumplidos los plazos y exigencias establecidas en la ley para que opere el derecho al olvido; ya que lo que no se encuentra permitido es su comunicación.

Por último, el artículo 1 transitorio de la ya mencionada ley 19.812 nos da un ejemplo claro del derecho al olvido, tanto desde un punto de vista temporal como de montos adeudados, al disponer que los responsables de los registros o bancos de datos personales que traten información señalada en el artículo 17 de la Ley 19.628, es decir, datos patrimoniales negativos comunicables, no podrán comunicarla cuando se refiera a obligaciones que, a la fecha de publicación de la ley, esto es 13 de junio de 2002, hayan sido pagadas o se hayan extinguido por otro modo legal. Asimismo, indica la norma que no podrán comunicar los datos relativos a esas obligaciones que se hayan hecho exigibles antes del 1 de mayo de 2002 y se encuentren

---

afectado por dicha información negativa, también puede producir un efecto positivo en la economía. Así, por ejemplo, si se trata de un empresario, una ley en tal sentido puede favorecer tal actividad, con el consiguiente beneficio para la economía…si la persona es simplemente un consumidor, la lógica es muy parecida, es conveniente para una economía de mercado que los consumidores sean el mayor número posible, y si uno de ellos ha salido de ella, puede ser altamente conveniente que después de transcurrido un determinado número de años tenga la posibilidad de volver a consumir ciertos productos o servicios, contribuyendo con ello a la demanda de dicha actividad económica."

[291] Antes de la modificación legal los plazos eran los siguientes: a) Para el caso de obligaciones no extinguidas, siete años desde que la respectiva obligación se hizo exigible. B) Para el caso de

impagas, siempre que el total de obligaciones impagas del titular que comunique el registro o banco de datos a la fecha de publicación de esta ley sea inferior a $2.000.000 por concepto de capital, excluyendo intereses, reajustes y cualquier otro rubro. Se establece, finalmente, con el objeto de impedir que se burle el espíritu de la ley, que en el caso de los incisos anteriores, tampoco podrá proporcionarse información al titular de los datos, ni comunicarse el hecho de que éste haya sido beneficiado con esas disposiciones.

2.6.3.6. Aclaración

La Ley 19.628 regula, asimismo, el procedimiento de aclaración en caso en que se efectúe el pago o se extinga la obligación por otro modo legal, estableciendo ciertas obligaciones para el acreedor y para el responsable del banco de datos respectivo. Así, si en el pago o la extinción de la obligación por otro modo legal ha intervenido directamente el acreedor, éste deberá avisar tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público[292] 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. En todo caso, 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.

A su vez, 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[293] del respectivo titular hasta que esté actualizada la información.

---

obligaciones pagadas o extinguidas por otro modo legal, tres años desde pago o desde su extinción por otro modo legal.

[292] La ley considera que aquellos bancos de datos que comuniquen datos patrimoniales negativos de los que trata el Título III de la ley son fuentes accesibles al público. Así, por ejemplo, Dicom o el Boletín de Informaciones Comerciales constituyen fuentes accesibles al público.

[293] El bloqueo de datos se encuentra definido en el artículo 2 letra b) de la Ley 19.628 como la suspensión temporal de cualquier operación de tratamiento de los datos almacenados, sin embargo, en la práctica el bloqueo de datos se asocia a la imposibilidad de comunicar los datos bloqueados.

La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16[294].

2.6.4. Datos personales sensibles.

La ley establece un concepto general y abierto de datos sensibles[295] en su artículo 2 letra g)[296], cuando señala que son aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad. Luego de lo cual, da una serie de ejemplos de datos sensibles, que en general, hacen suyo, la categorización que de ellos se hace en derecho comparado[297]:

- Los hábitos personales.
- El origen racial.
- Las ideologías y opiniones políticas.
- Las creencias o convicciones religiosas.

[294] Procedimiento de hábeas data contemplado en la ley.

[295] "En seguida, siguiendo a la legislación española, optó por una definición amplia de los datos de carácter personal, como aquellos referidos a cualquier información relacionada con personas naturales, y entendió por 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." Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2093. 05 de agosto de 1998.
Rodolfo Herrera ha criticado con razón este concepto amplio de datos sensibles, señalando que "El concepto que da la Ley nos parece muy amplio, por lo que normalmente será el juez quien tenga que interpretar en cada caso particular si el dato es o no sensible, y, por lo tanto, su tratamiento está prohibido *a priori* salvo en las excepciones que fija esta ley. En tal sentido, la normativa sobre datos sensibles operará en muchos casos discutibles sólo una vez generado el conflicto jurídico, ya que la primera calificación la efectuar el responsable del registro, quien normalmente tendré una pretensión diametralmente opuesta a la del titular del dato, ya que a aquél le interesará tratar dicha información con exigencias menores a las que se aplican a los datos sensibles". HERRERA, Rodolfo. s/a. Análisis de la ley chilena Nº 19.628, sobre protección a la vida privada, de 28 de agosto de 1999.

[296] Art. 2 g) Ley 19.628: "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."

[297] El considerando 33 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, reconoce esta categoría especial de datos personales estableciendo que: "los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales." A su vez, el artículo 8.1 de la señalada directiva indica que: "Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad."

- Los estados de salud físicos o psíquicos.
- Y, finalmente, la vida sexual.

La característica esencial de los datos sensibles es que se encuentran protegidos con mayor fuerza que los otros tipos de datos que se establecen en la ley, ya que su tratamiento queda condicionado a que concurra alguna de las tres hipótesis taxativas previstas en el artículo 10 de la Ley 19.628[298], esto es: que una ley lo autorice, que exista consentimiento del titular de los datos, o cuando su procesamiento sea necesario para determinar u otorgar beneficios de salud que correspondan a sus titulares. De manera que la regla general respecto de esta clase de datos es la prohibición de ser objeto de tratamiento, ocupando la autorización del titular de los datos una importancia superior que en los otros tipos de datos que se han analizado, ya que respecto de los datos personales sensibles no se han establecido en la Ley 19.628 excepciones que legitimen su tratamiento sin autorización de su titular[299].

2.6.5. Datos personales sensibles de salud.

Los datos personales de salud son considerados por la ley como datos sensibles, ya que al definir este último concepto se hace referencia a los estados de salud físicos y psíquicos de las personas y luego se excepciona de la regla general, en el artículo 10 de la ley, de la autorización previa legal o convencional que opera respecto de este tipo de datos, a aquellos datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. De manera que respecto a este tipo de datos, no se requiere la autorización del titular de ellos para efectuar tratamiento.

Esta excepción fue incluida en la ley a partir de las sugerencias efectuadas por Asociación de Isapres A.G., y el Fondo Nacional de Salud. La Asociación de Isapres señaló que resultaba preocupante para su actividad la circunstancia de que se consideren datos sensibles -y, por lo tanto, se restrinja su tratamiento a los casos en que la ley lo autorice o exista consentimiendo del interesado-, los estados de salud síquicos o físicos de las personas.

[298] Art. 10 Ley 19.628: "No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares."

Manifestó dicha entidad que el sistema de salud privado previsional requiere, para una adecuada y eficiente administración, del conocimiento y, eventualmente, el manejo de determinados datos de sus afiliados. No tener acceso a antecedentes de los beneficiarios podría impedir, por ejemplo, el control del fraude en las licencias médicas, evaluación de las enfermedades preexistentes reconocidas legalmente, programas preventivos de salud, y otras materias que inciden en el buen funcionamiento de este sistema. En virtud de tales razonamientos, dicha institución sugirió que se permita que los datos relativos a los estados de salud de las personas puedan tratarse, respetando la confidencialidad que estas materias lógicamente deben tener, por instituciones públicas o privadas que deban determinar el otorgamiento de beneficios a sus adherentes.

De su parte, el Director del Fondo Nacional de Salud, advirtió que la excepción al tratamiento de los datos sensibles no debiera limitarse sólo a los estados de salud de las personas, pues la propia definición de datos sensibles, unida a lo que se entiende por datos personales, no permite con certeza asegurar que sólo los datos sobre estados de salud serán necesarios para determinar los beneficios que una persona o grupo de personas debiera recibir. Explicó que la necesidad de que se contemple el estado de salud de las personas para la determinación de los beneficios es un elemento altamente relevante, pero existen otros datos que también son requeridos para una correcta planificación de los beneficios a entregar determinando los grupos o segmentos de población, tanto en su caracterización epidemiológica y demográfica como en el tipo de intervención a realizar. Así, por ejemplo, para un programa de Sida, es necesario trabajar con una serie de datos respecto de las personas, los cuales obviamente incluyen conductas sexuales, estados de salud y otros, o bien, para analizar un problema de salud mental, los datos requeridos obviamente se referirán a conductas de vida y severidad del caso. Es necesario trabajar también con alguno de los datos sensibles cuando se estructuran grupos de riesgo de la población en términos de prevalencia de enfermedades, tales como el sexo o la raza de las personas, lo cual es altamente relevante para la correcta determinación de los beneficios que se van a otorgar a cada grupo. Por estas consideraciones, propuso que se pudieran tratar aquellos datos sensibles que se relacionen con la determinación u otorgamiento de los beneficios que corresponda a sus titulares, de esa manera, se podrían tratar todos los datos sensibles que se relacionen con alguna de esas dos finalidades.

[299] Salvo el caso de los datos que denomino datos personales sensibles de salud, que se tratan a continuación.

La Comisión Mixta se manifestó partidaria de esa proposición, de forma tal que incluyó como circunstancia excepcional que permite el tratamiento de datos sensibles, además de la autorización legal o el consentimiento del titular, cuando sean necesarios para la determinación u otorgamiento de beneficios que correspondan a sus titulares. Prefirió añadir, con todo, que debe tratarse de beneficios "de salud", a fin de acotar la habilitación que se concede, que de otra forma se establecería en términos excesivamente amplios[300].

2.6.6. Datos personales médicos.

La Ley 19.628 modificó a través de su artículo 24, el artículo 127 del Código Sanitario, mediante la incorporación de los siguientes incisos segundo y tercero: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo"[301]. 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."[302]

---

[300] Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 137. 02 de junio de 1999.

[301] El Libro X del Código Sanitario, que se denomina "De los procedimientos y sanciones" consulta tres títulos. De acuerdo al primero, se regula la inspección y allanamiento a que está facultada la autoridad sanitaria para la debida aplicación de las disposiciones del Código y su reglamento, y de los decretos y resoluciones del Director de Salud; de acuerdo al segundo se reglamenta el sumario sanitario, que es el procedimiento que se contempla para el conocimiento de las infracciones a dichas normas; y finalmente, de acuerdo al tercero, se regulan las sanciones y las medidas sanitarias. La primera, por norma general, va de un décimo de unidad tributaria mensual a 1000 unidades tributarias mensuales; las segundas, que pueden ir asociadas a la sanción pecuniaria, consisten en la clausura de establecimientos, edificios, casas, locales o lugares de trabajo donde se cometiere la infracción; la cancelación de la autorización de funcionamiento o de los permisos concedidos; la paralización de obras; y el comiso, destrucción y desnaturalización de productos, cuando proceda.

[302] Esta norma fue incluida a petición del Ejecutivo. "El contenido de esta propuesta recoge otra iniciativa de ley, cuyo objeto es garantizar la reserva de las recetas médicas, ya aprobada por el honorable Senado, que se encuentra actualmente en segundo trámite constitucional en la honorable Cámara de Diputados. (Boletín Nº 1985 -11), y es complementaria de las normas aprobadas en los artículos 2º, letra g), y 10 por la Comisión Mixta, que en general dan a los datos de salud la calidad de datos sensibles". Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 137. 02 de junio de 1999.

Se puede colegir de la sola lectura del anterior texto legal, que en este tipo de datos el control que posee el titular de ellos es mucho mayor que en las categorías de datos que llevamos revisadas, respecto a la posibilidad de comunicación ya que sólo el titular puede autorizar la revelación de sus datos personales médicos. No obstante lo anterior, podría argüirse que al ser este tipo de datos sensibles, y por lo tanto, aplicarse respecto de ellos lo señalado en el artículo 10 de la ley, estos datos podrían ser tratados y comunicados si existiese autorización legal o fueran necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares, sin que medie autorización previa del titular de los datos. Creemos que lo anterior no es posible, ya que claramente el artículo 24 que modificó el Código Sanitario en los términos expuestos constituye una norma especial, y por lo tanto, para las hipótesis por ella reguladas sólo cabe la autorización del titular de los datos, en este caso, del paciente.

Además, se facultó a las farmacias para dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos, sin embargo, en ningún caso la información que proporcionen consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos, es decir, se trata acá de datos disociados o estadísticos.

Finalmente, se plantea a propósito de los datos o información consignada en las recetas médicas, una interesante discusión: la receta médica constituye un documento que está compuesto no sólo de datos personales que se refieren al paciente al cual el médico prescribe los medicamentos contenidos en ella, sino que también, contiene datos personales del médico que prescribió la receta. Ante esta situación cabe preguntarse, en base a lo señalado en el inciso primero del artículo 24 ¿La autorización que otorga el paciente para revelar o copiar el contenido de la receta, legitima el tratamiento de datos que le conciernen al médico que la prescribió? Caben acá, dos hipótesis, a saber: señalar que sí lo legitima por que el texto legal no distingue, y consecuentemente todo el contenido de la receta –incluyendo los datos del médico-, previa autorización del paciente, puede ser tratado y revelado, o bien, señalar que sólo pueden tratarse aquellos datos que le conciernen al paciente autorizante, pero no los datos personales del médico, ya que éstos le pertenecen, y consecuentemente se requiere, para el tratamiento de esta información, también de su consentimiento. Ante el vacío de la norma que no resuelve el problema planteado, creemos que en base a las reglas generales de la Ley 19.628 que establecen

que el titular de los datos, y no otra persona, deben entregar su autorización para el tratamiento, la segunda hipótesis planteada es la correcta, esta interpretación es además, armónica con la historia de la ley, ya que al votar el artículo en comento en el Congreso, se optó por entregar reserva a los datos del médico[303].

2.6.7. Datos personales públicos.

A los efectos de la clasificación que efectuamos de los datos personales que reconoce la Ley 19.628, denominaremos datos personales públicos, a aquellos datos que son tratados por organismos públicos en tanto titulares de registros o bancos de datos. La señalada normativa contiene un título especial, el Título IV "Del tratamiento de datos por organismos públicos" compuesto por tres artículos, que establece algunas normas específicas referentes al tratamiento de datos personales en el ámbito público. Las cuales será analizadas a continuación[304].

El artículo 20 de la Ley señala que: "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."

---

[303] "En el seno de la Comisión Mixta se debatió con amplitud, en particular, la reserva que se impone respecto del nombre de los médicos que expiden las recetas.
Algunos de sus integrantes se manifestaron contrarios a establecer la reserva, y por ende, prohibir la divulgación del nombre del médico que expidió la receta, ya que no encontraron justificación suficiente para su exclusión. Precisaron que, al interior de nuestra sociedad, se desarrolla una serie de actividades que pueden generar diversos inconvenientes para quienes la ejercen, pero de ello no se deduce que deba establecerse a su respecto una suerte de anonimato, como no ocurre respecto de los abogados, que suscriben y se responsabilizan de sus presentaciones judiciales, y de los propios magistrados, que pueden llegar a castigar a una persona a la pena de muerte, bajo su firma, lo que es de público conocimiento. Añadieron que, desde un punto de vista práctico, la falta de publicidad impedirá conocer el grado de actualización de los listados de productos farmacéuticos que tenga el médico que los prescribe, lo que podría tener incidencia en el mejor tratamiento de sus pacientes.
Otros integrantes de la Comisión Mixta, en cambio, se manifestaron en favor de establecer esta reserva, por estimar que constituye una herramienta adecuada para cautelar un mejor ejercicio de la profesión médica. En efecto, agregaron, para una determinada enfermedad siempre existen diferentes alternativas, desarrolladas por otros tantos laboratorios. El hecho de permitir la difusión del nombre de los médicos que recetan determinados productos pudiera originar una actuación inconveniente de algunos laboratorios respecto de ellos, a fin de inclinarlos a prescribir sus propios medicamentos. Argumentaron que, de esta forma, se garantiza la libertad profesional para decidir cuál es la mejor alternativa para el paciente.
Al ser sometida a votación ambas opciones, se pronunciaron por establecer la reserva de la identidad de los médicos los honorables Senadores señores Larraín y Zurita y los honorables Diputados señores Bartolucci y Tuma. En cambio, lo hicieron por la publicidad de sus identidades los honorables Diputados señores Cardemil, Elgueta y Ojeda, absteniéndose el honorable Senador señor Viera-Gallo. Por incidir la abstención en el resultado, se repitió la votación, sumándose en esta oportunidad el honorable Senador señor Viera-Gallo a la posición de la mayoría". Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 138. 02 de junio de 1999.

Como podemos observar, se establece para los organismos públicos un tratamiento diferenciado al que se efectúa respecto de los privados, ya que se les permite actuando dentro de su competencia, y por supuesto, en tanto se respete la normativa, tratar datos sin consentimiento del titular[305]. Lo anterior, implica que en esta categoría de datos la autorización previa del titular de los datos para efectuar tratamiento de ellos, en principio, no se requiere, pues es de suyo propio que los órganos públicos actúen dentro de su competencia[306]. Por lo demás, así ha operado en la práctica; los organismos públicos efectúan los más diversos tratamientos de datos personales, esgrimiendo que lo efectúan dentro de su competencia, ya sea por que así lo ha interpretado la Contraloría General de la República en su momento[307], o bien, porque existe ley

---

[304] El artículo 21 se estudiará a propósito de los datos personales penales, en el siguiente acápite.

[305] Respecto del régimen especial que establece la Ley 19.628 en el Título VI cabe señalar que a los organismos públicos se les aplican todas las normas establecidas en la ley, salvo en lo que se encuentren modificadas por las normas especiales del señalado título, que por su carácter de especialidad rigen por sobre las normas generales. Esta interpretación se corrobora por lo indicado en el Informe de la Comisión Mixta, cuando señala que: "La segunda parte de la disposición, que somete el tratamiento de datos personales que hagan los organismos públicos "a las reglas precedentes", deja de manifiesto que -como anticipó el artículo 1º, inciso primero-, son unos mismos los preceptos que se aplican a los organismos públicos y a los particulares. No hay regulaciones separadas y diferentes, que permitan a unos inmiscuirse en mayor medida que a los otros en aspectos que conciernen tan estrechamente a las garantías constitucionales de respeto y protección a la vida pública y privada y a la honra de la persona y de su familia. Las normas contenidas en este título, por consiguiente, son especiales, pero sólo en cuanto recaen sobre aspectos propios del sector público." Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 131. 02 de junio de 1999.

[306] Así también pareció entenderlo el legislador cuando señala que "La primera parte de este artículo (el artículo 20), que deja sujeto el tratamiento de datos personales por parte de un organismo público a aquellos que se refieran a materias de su competencia, encuentra su origen en el artículo 6º de la honorable Cámara de Diputados, que establecía que el tratamiento de datos "sólo será admisible cuando sea indispensable para el cumplimiento de las tareas que les corresponden y dentro del ámbito de su competencia", y en el artículo 19, Nº 1, del texto preparado durante el tercer trámite constitucional, conforme al cual "el tratamiento de datos debe efectuarse dentro del ámbito de la competencia legalmente determinado del respectivo organismo". Si bien es una norma que puede estimarse innecesaria, al tenor del artículo 7º de la Constitución Política, presta utilidad su inclusión en un cuerpo legal que, por primera vez, da reglas en forma sistemática sobre los datos personales, más aún si se considera que numerosos organismos públicos tienen solamente normas de rango reglamentario sobre la materia o, incluso, ni siquiera de esa jerarquía." El paréntesis es nuestro. Ibídem.

[307] El dictamen número 43.866 de fecha 03.10.2003 de la Contraloría General de la República indica que: "En virtud de las facultades que le confiere al Servicio de Tesorerías el artículo 9, letra b, número 4, de su Estatuto Orgánico, para celebrar contratos relacionados con el cumplimiento de los fines del mismo, se encuentra habilitado para suscribir, con empresas especializadas que manejan bases de datos, acuerdos de voluntades para intercambiar información relativa a contribuyentes y deudores que se encuentren en mora con el Fisco, dado que tal información no tiene el carácter de secreta o reservada, sino que es pública. La información de que se trata se genera por el propio Estado, con motivo de su actividad que es pública, toda vez que, como se ha visto, está referida a aquellas deudas tributarias o créditos morosos del sector público que se encuentran en proceso de cobranza por el Servicio de Tesorerías, conforme a las atribuciones que le confieren al efecto las normas consignadas en el Decreto Ley 1.263, de 1975, y en el Código Tributario." Ver en el mismo sentido, jurisprudencia de la Contraloría General de la República respecto de la posibilidad de las Municipalidades para suscribir convenios con empresa privadas que administren bases de datos de datos, con el objeto de incorporar a dichas bases, las nóminas de deudores morosos, por conceptos de derechos o patentes municipales. (dictamen número 42.760 de fecha 16.11.2001 de la Contraloría General de la República) y respecto de las atribuciones con que cuenta el Servicio de Impuestos

expresa que los autoriza a tratar datos personales, respecto a esto último, la técnica legislativa, que se ha estado utilizando en las últimas leyes dictadas en el ámbito de las competencias de ciertos organismos públicos, es entregarles a éstos, expresamente la atribución o función (competencia) para tratar datos personales. Así por ejemplo, en la ley que establece la Autoridad Sanitaria Nº 19.397, en su artículo 4 numeral 5 se señala que será función del Ministerio de Salud: "Tratar datos con fines estadísticos y mantener registros o bancos de datos respecto de las materias de su competencia. Tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud. Para los efectos previstos en este número, podrá requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuere necesaria. Todo ello conforme a las normas de la ley N° 19.628 y sobre secreto profesional"[308].

No obstante lo señalado anteriormente, cabe preguntarse respecto de la redacción del artículo 20 de la ley, cuándo los organismos públicos actúan dentro de su competencia y qué pasa con el tratamiento de datos que se efectúa por los organismos públicos fuera de su competencia.

Respecto al primer punto, compartimos el criterio que indica que los órganos públicos actúan dentro de su competencia, en la medida que dicha actuación se ejecute de acuerdo a las funciones, facultades y atribuciones que determine el ordenamiento jurídico[309]. De esta manera, no hay duda en que un determinado organismo público actúa dentro de su competencia al tratar datos personales, si existe texto legal expreso que lo autorice a efectuar el referido tratamiento. El problema se presenta cuando tal texto no existe y se deben interpretar las funciones y/o

---

Internos para suscribir convenios con empresas de tecnología automatizada de información, en virtud de los cuales, el referido Servicio puede tener acceso a las bases de datos de dichas empresas en aquellos aspectos que son de su interés, y las referidas empresas pueden, a su vez, acceder a ciertos y determinados datos con que cuenta esa entidad pública: número de rol único tributario de los contribuyentes, nómina de contribuyentes con incumplimiento tributario, avalúos de bienes raíces, tasación de vehículos, y timbraje de documentos, que permite verificar la validez de la documentación tributaria (dictamen número 10.322 de fecha 21.03.2001 de la Contraloría General de la República).

[308] Ver también Ley N° 19.891. 2003. Crea el consejo nacional de la cultura y las artes y el fondo nacional de desarrollo cultural y las artes. Agosto 2003, que indica en su artículo 3 número que es función del Consejo: Desarrollar y operar un sistema nacional y regional de información cultural de carácter público. Para la operación del sistema nacional y regional de información cultural a que hace referencia este numeral, el Consejo podrá crear un banco de datos personales de aquellos señalados en la ley Nº 19.628.

[309] "Derecho Constitucional". Tomo I. 1997. Por Emilio Pfeffer "et al". 2ª ed. Santiago de Chile, Editorial Jurídica de Chile. 375 p.

atribuciones que le entrega la ley a un determinado órgano público para poder encuadrar dentro de ellas el efectuar tratamiento de datos personales tomando en cuenta una serie de elementos, como por ejemplo: la naturaleza del dato, la finalidad que se persigue con el tratamiento, la función que cumple el referido órgano público al efectuar el tratamiento de datos de que se trate. De esta manera, no es posible, dado el estado actual de la legislación, establecer un principio general de legitimidad para el tratamiento de datos por parte de organismos públicos. Serán los Tribunales de Justicia y al Contraloría General de la República, entonces, los llamados a pronunciarse respecto a la actuación de un organismo público dentro de su competencia en tanto responsable de un banco de datos[310].

Respecto a la segunda pregunta, y a partir de la lectura del artículo en comento, se pueden concluir dos cosas:

- Que aquél tratamiento es ilegal (sobre todo teniendo en cuenta el espíritu declarado de la ley) y no se puede realizar bajo ningún supuesto por la utilización del vocablo "sólo".
- Que se puede efectuar el tratamiento fuera de la competencia del órgano, pero se requerirá en ese caso, consentimiento del titular.

Creemos que dada la historia de la ley[311] y dado el principio general por el cual cualquier tratamiento de datos es legítimo en la medida en que sea autorizado por el titular o por la ley y se

[310] En este sentido se ha pronunciado la Controlaría General de la República en los dictámenes mencionados más arriba, al señalar que: "cabe agregar que la sola circunstancia de que un servicio público efectúe tratamiento de datos personales materia regulada en el referido cuerpo legal y entendida como cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que, en general, le permitan el manejo más eficiente de la informaci6n que tiene a su cargo-, no implica que el respectivo servicio público se encuentre facultado para ceder esos datos a terceros. Esta última posibilidad debe ser analizada a la luz de la naturaleza de la información que pretende cederse y de las competencias que desarrolla el órgano pertinente".

[311] Analizando la historia de la ley respecto de este precepto, se observa que su evolución tendió a ser menos restrictiva y exigente en cuanto a los requisitos de legitimidad para efectuar tratamiento de datos por parte de organismos públicos, así en un principio cf., Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2129. 05 de agosto de 1993, se establecía en el artículo 19 del proyecto que "El almacenamiento o tratamiento de datos personales por parte de organismos públicos se ajustará a las reglas que siguen: 1. El tratamiento de datos debe efectuarse dentro del ámbito de la competencia legalmente determinado del respectivo organismo y contando con autorización legal para ello. 2. Tal tratamiento debe ser necesario para el cumplimiento de tareas que le correspondan o para resguardar el orden y seguridad públicos, o la pronta y cumplida administración de justicia, o debe redundar en beneficio del titular de los datos." Luego, cf. Diario Sesiones del Senado. Sesión 2, tomo 60, pág. 131. 02 de junio de 1999, se deja constancia de la propuesta efectuada por el Ejecutivo en orden a reemplazar el antiguo artículo 19 por un nuevo artículo 20 que establecía que 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, texto que en definitiva, fuera aprobado por los legisladores.

cumpla con la normativa que establece la Ley 19.628, la segunda interpretación es la correcta. La jurisprudencia aun no se ha pronunciado sobre este punto específico.

Finalmente, el artículo 22 de la ley establece la existencia de un registro de los bancos de datos personales a cargo de organismos públicos, el que será llevado por el Servicio de Registro Civil e Identificación. 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[312]. 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 anteriormente dentro de los quince días desde que se produzca.

Si bien la norma parece tener sentido y ser de utilidad para los titulares de datos, ya que a partir del registro podrían saber qué organismos públicos tratan su datos, la realidad, es que muy pocos órganos del Estado han cumplido con esta norma[313], no pudiendo el Servicio de Registro Civil obligarles a cumplirla, ya que carece de facultades de fiscalización en ese sentido[314].

2.6.8. Datos personales penales.

Respecto a esta categoría de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias que he denominado datos personales penales, el artículo 21 de la Ley señala que los organismos públicos que sometan a tratamiento los señalados datos, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. Haciendo excepción a esta regla los casos en que esa información les es solicitada por los Tribunales de Justicia u otros organismos públicos dentro

[312] El Reglamento está contenido en el Decreto 779 que aprueba Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos, publicado en el Diario Oficial el 11 de noviembre de 2000.
[313] Para revisar los órganos públicos que han cumplido esta obligación. Visitar http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html
[314] Algunos autores nacionales, han criticado con razón, esta ausencia de facultad de fiscalización por parte del Servicio de Registro Civil. JIJENA, Renato. op cit. pág. 96 y CERDA, Alberto., op. cit. pág. 94.

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. Es decir, que respecto a este tipo de datos la autorización del titular para efectuar su tratamiento no cumple ningún rol, pues es la propia ley la que autoriza al Servicio de Registro Civil e Identificación a llevar un registro de este tipo de datos[315].

De lo señalado, cabe preguntarse si el titular de los datos se encuentra facultado para solicitar antes de que se encuentre prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, se le comuniquen sus datos personales penales. Al respecto, la Contraloría General de la República se pronunció respondiendo una consulta efectuada en este sentido por el Servicio de Registro Civil e Identificación, señalando que: "de acuerdo a lo informado por el servicio los certificados de antecedentes con arreglo a la normativa sólo se expiden al titular o a determinadas autoridades públicas, lo que no pudo sino tenerse en cuenta por el legislador al establecer la disposición, es preciso entender que el beneficio que contempla el articulo 21 en examen -destinado a impedir que terceros puedan tomar conocimiento de la información obligando al servicio a no comunicar los datos- sólo puede tener eficacia práctica en tanto esa entidad omita en los aludidos certificados la información correspondiente. Por consiguiente, de conformidad con lo expuesto, es menester concluir que el beneficio establecido en el artículo 21 de la ley Nº 19.628 importa que en la medida en que concurran las circunstancias que indica, en los certificados de antecedentes que expide el Servicio de Registro Civil e Identificación deben omitirse los datos personales que la misma norma señala. Es necesario consignar, finalmente, y en armonía con lo señalado en forma previa, que ello no obsta al derecho del titular para exigir del mismo servicio información acerca de los datos relativos a su persona en los términos del Título II de la ley -artículos 12 al 16- y para, en su caso, obtener la modificación, eliminación o bloqueo de sus datos personales, de tal modo que si el titular exige la información en ejercicio específico de aquel derecho, el Servicio de Registro Civil e Identificación debe proceder con arreglo a lo establecido en dicho Título II."[316]

[315] CHILE. 1925. Decreto Ley N° 645 sobre el Registro Nacional de Condenas. Octubre 1925.
[316] Contraloría General de la República. Dictamen acerca de los certificados de antecedentes y el artículo 21 de la ley n° 19.628, sobre protección de datos de carácter personal. REF: 34565/99 del 25 de octubre de 2000.

Cabe resaltar, por último, que este tipo de datos puede seguir tratándose, en cualquiera de sus formas, luego de que concurran las circunstancias que indica el artículo 21, lo que no se puede efectuar, y por ende constituye infracción a la ley, es comunicar los datos referentes a condenas cuya acción penal o pena se encuentre prescrita o cumplida, respectivamente[317].

2.6.9. Datos personales en general.

Por último, como una clase residual de datos contemplamos todos aquellos datos personales que no caben dentro de ninguna de las categorías esbozadas anteriormente, a éstos, les denominamos datos personales en general, respecto de ellos, se aplica el principio general que se establece en el inciso primero del artículo 4 de la ley, de manera que su tratamiento sólo podrá efectuarse cuando otras disposiciones legales distintas de la Ley 19.628 lo permitan[318] o el titular consienta expresamente en ello. De manera, que la autorización del titular sí tiene relevancia en este tipo de datos personales a los efectos de establecer la licitud de un determinado tratamiento de datos personales.

2.6.10. Resumen

Como se puede colegir de la lectura de este acápite, la Ley 19.628 reconoce diversas categorías de datos personales que en han sido clasificadas en la presente tesis alejándose de los criterios tradicionales de clasificación, ya que se ha tomado como elemento distinguidor entre ellos, el mayor o menor control que el titular de los datos posee sobre éstos, control que se ejerce a través de la autorización para su tratamiento. A continuación elaboramos un cuadro resumen que nos muestra los distintos tipos de datos personales analizados bajo el prisma ya esbozado.

---

[317] Operando respecto de este tipo de datos el mismo tratamiento legislativo que para los datos patrimoniales negativos del Título III.

[318] No consideramos acá la hipótesis relativa a la autorización que da la propia Ley 19.628, ya que ésta se encuentra contemplada en las diversas categorías de datos que ya se analizaran.

TABLA Nº 2

"Cuadro Resumen Clasificación Datos Personales"

Categoría de Dato Personal	Dato personal proveniente fuentes accesibles al público	Dato personal tratado por personas jurídicas privadas	Dato personal relativo a obligaciones de carácter económico, financiero, bancario o comercial.	Dato personal sensible	Dato personal de salud sensible	Dato personal médico	Dato personal público.	Datos personal penal	Dato personal en general
Autorización del Titular	NO	NO	NO	SI*	NO	SI	NO**	NO	SI*

* Sin embargo también el tratamiento puede ser autorizado por una norma legal.

** Sólo se requiere autorización cuando el órgano público actúa fuera de su competencia en el tratamiento de los datos.

2.7. De los derechos subjetivos otorgados al titular de los datos.

2.7.1. Cuestiones preliminares.

La Ley 19.628 establece una serie de derechos subjetivos[319] que tienen como fin último entregar las herramientas legales necesarias al titular de los datos personales con el objeto de que éste pueda ejercer un control efectivo respecto a la información de naturaleza personal que le concierne y que es tratada por terceros[320].

[319] Compartimos la opinión de Hernán Corral, en el sentido de entender que los derechos que establece la Ley 19.628 para el titular de los datos, son derechos subjetivos, esto es, facultades morales que permiten a su titular exigir de otra persona una determinada conducta. CORRAL, Hernán. De los derechos de las personas sobre los responsables de bancos de datos: el hábeas data chileno. EN: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5, 2001. pp. 39-59.

[320] A este respecto la Ley 19.628 cumple con los requerimientos establecidos por la OCDE en el documento denominado "Directrices de la OCDE sobre Protección de la privacidad y flujos transfronterizos de datos personales". OECD Guidelines on the Protection of privacy and transborder flows of personal data. 2001. y con los señalados por la ONU, en el documento denominado "Principios rectores para la reglamentación de los ficheros computadorizados de datos personales". Guidelines for the regulation of computerized personal data files. 1990. En este sentido se pronuncia Pablo Palazzi, cuando señala que "es decir, aparentemente la ley otorga tanto un recurso para proteger los derechos de acceso y corrección y los restantes otorgados por la ley, así como también indemnizaciones morales y materiales. En estos aspectos la norma satisface los recaudos establecidos por la Directiva". PALAZZI, Pablo. op. cit. pág, 192.

Los derechos de los titulares de datos reconocidos en nuestra normativa protectora de datos, se encuentran establecidos básicamente en el Título II de la ley "De los derechos de los titulares de datos", que ocupa los artículos 12 al 16[321]. Estos derechos son:

- El derecho de acceso o información.
- El derecho de modificación o rectificación.
- El derecho de cancelación.
- El derecho de bloqueo.

Antes de entrar a revisar el contenido de cada uno de ellos, me referiré a algunos puntos de importancia tratados por la ley, y que dicen relación con el ejercicio de estos derechos.

2.7.1.1. Legitimación para ejercer estos derechos:

El legitimado para ello es el titular de los datos, el afectado. El problema que surge es saber si estos derechos pueden ser ejercidos a través de representante, ya sea legal o voluntario. La Ley guarda silencio en este punto. Debido a ello, surgen dos alternativas: La primera es señalar que se trata de un derecho personalísimo y que, por ende, sólo puede ser ejercido por el titular de los datos, sin que pueda existir representación de por medio. Y la segunda alternativa, es señalar que sí se puede ejercer este derecho por medio de representantes. Creemos que la primera opción no es la correcta, por varios motivos.

En primer lugar, porque la finalidad de la ley es justamente brindar protección a los titulares de datos personales, amparo que no podría llevarse a cabo en aquellas hipótesis de imposibilidad de ejercicio personal de los derechos. Imaginemos una persona que se encuentre fuera del país, o incluso el caso de un menor de edad, ¿Es lógico y congruente con la Ley, que no puedan ejercer sus derechos, por estar imposibilitados de ser representados legítimamente por otro?, la respuesta a este cuestionamiento es rotunda: no.

En segundo término, negar la posibilidad de ejercicio mediante representante o mandatario, contraría las normas y principios generales que sobre representación existen en nuestro ordenamiento, que nos señalan que todo acto puede celebrarse a través de mandatario o representante, salvo los casos que la propia ley exceptúa, como por ejemplo, en el testamento.[322]

Finalmente, hay una razón de texto, el artículo 12 inciso 5 de la Ley 19.628 señala que: "El derecho de copia gratuita sólo podrá ejercerse personalmente", lo que nos lleva a concluir, a *contrario sensu*, que el resto de los derechos pueden ser ejercidos a través de representantes, ya que cuando el legislador quiso indicar la existencia de un derecho personalísimo así lo hizo.

Por estas razones, es que creemos que sí procede la representación en el ejercicio de estos derechos. En todo caso, ella debe ser formalizada a través de medios adecuados que permitan garantizar la existencia de la representación. Así, por ejemplo, en el caso de tratarse del ejercicio de un derecho de acceso a datos personales de un menor de edad, podrá ser ejercido por el padre o madre, en tanto éstos prueben el vínculo de parentesco, lo que en términos simples se efectuará a través de las correspondientes partidas o actos de reconocimiento. En el caso que estemos en presencia de una representación voluntaria, ésta podrá ser probada a través de escritura pública, o bien de un instrumento privado autorizado ante Notario.

2.7.1.2. Gratuidad en el ejercicio de los derechos

Otro principio importante que se establece es el de la gratuidad en el ejercicio de estos derechos. Así, el artículo 12 señala que la información, modificación o eliminación de los datos serán absolutamente gratuitas. Hacemos hincapié en que se omite mencionar el bloqueo, de lo que se colige que el ejercicio de este derecho de bloqueo puede estar sujeto a cobro, que en todo caso, nunca podrá ser de tal entidad que imposibilite su ejercicio, es decir, debe ser un cobro racional y proporcional.

---

[321] El artículo 16 regula la acción de hábeas data, que no constituye un derecho subjetivo sino que la vía procesal para hacer efectivos judicialmente los referidos derechos. Por lo que será considerada en otra parte de este acápite.

[322] Art. 1448 Código Civil. "Lo que una persona ejecuta a nombre de otra, estando facultada por ella o por la ley para representarla, produce respecto del representado iguales efectos que si hubiese contratado él mismo."

2.7.1.3. Inalienabilidad

El artículo 13 de la Ley señala que el derecho de los titulares a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

De esta manera, cualquier cláusula, acto, convención, contrato, declaración de voluntad unilateral, que esté destinada a limitar o a suprimir el ejercicio de estos derechos será nula absolutamente por objeto ilícito, en relación con el artículo 10 del Código Civil, que señala que los actos prohibidos por la ley son nulos y de ningún valor. De más está señalar la utilidad de esta norma, que impide que, por ejemplo, a través de contratos de adhesión -que usualmente no son leídos con mucha profundidad por la parte más débil en la contratación- se establezcan cláusulas en donde el titular de datos renuncie o limite sus derechos.

2.7.1.4. Principio de calidad de los datos.

Finalmente, cabe mencionar como una norma importante en relación con la materia que nos ocupa el artículo 6 de la Ley, cuyo contenido es una aplicación del principio de calidad de los datos. Este artículo indica en su inciso final que 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. De manera, que en el evento que se dé alguna de las hipótesis que establece la ley para que proceda la eliminación, la modificación o el bloqueo de los datos, y el responsable del registro no lo hiciera, está claramente cometiendo una infracción a la ley, ya que se establece como una obligación para él realizar tal proceder.

Ya revisados estos principios fundamentales, se revisará a continuación el contenido de cada uno de los derechos subjetivos reconocidos en la Ley al titular de los datos.

2.7.2. Derechos protegidos.

2.7.2.1. El derecho de información.

Es el derecho que posee todo titular de datos para exigir del responsable del banco de datos ya sea privado o público, información que le permita saber si se tratan datos suyos y, de ser así, cerciorarse de su exactitud y de la licitud de su tratamiento[323].

Este derecho de información constituye la puerta de entrada al ejercicio de los demás derechos, pues sólo si se tiene información o conocimiento sobre si se están tratando datos personales y de qué manera se está haciendo, se podrá saber si se está respetando el principio de calidad y finalidad en el tratamiento, y así exigir, en el evento que así procediese, su eliminación, cancelación o bloqueo.

---

[323] Durante la tramitación del proyecto de ley de que se trata, se utilizó en forma indistinta el concepto de derecho de acceso y derecho de información, respecto a este derecho que se encuentra regulado en el artículo 12 y que comentamos. Sin embargo, en estricto rigor, cabe distinguir, tal como lo efectúa la doctrina y el derecho comparado entre derecho de acceso y derecho de información. Así, por ejemplo, la Directiva Europea que regula la materia, establece en su artículo 10, bajo el epígrafe derecho de información, que "el responsable del tratamiento o su representante deberán comunicar a la persona de quien recaben los datos que le conciernen, por lo menos la información que se enumera a continuación, salvo si la persona ya ha sido informado de ello a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: - las categorías de los datos de que se trate. - los destinatarios o las categorías de destinatarios de los datos, - la existencia de derechos de acceso y rectificación de los datos que la conciernen", regulando la propia directiva, luego en el artículo 12 el derecho de acceso al interesado, estableciendo que: "Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; - la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado." De lo estatuido por la Directiva Europea, se puede colegir que las diferencias entre ambos conceptos son básicamente dos: en primer lugar, el derecho de información constituye un concepto más amplio que el derecho de acceso, ya que lo incluye, pues el responsable del fichero debe informar sobre la existencia del derecho de acceso y en segundo lugar, como lo señala Alberto Cerda, en cuanto a que la distinción entre el derecho de información y de acceso está dada en el hecho que el primero se concreta mediante el registro de las bases de datos que permite a toda persona cerciorarse de quiénes, qué y para qué procesan datos nominativos; en tanto que el segundo, se concibe como requerimiento concreto del titular ante el responsable de la base de datos, a fin de

Este derecho se traduce en la posibilidad de efectuar una serie de preguntas o cuestionamientos al responsable del registro o banco de datos. Así, el titular de los datos tiene derecho a informarse acerca de:

- Si un determinado banco de datos contiene información relativa a su persona.
- El contenido de la información relativa a su persona que posee el responsable del banco de datos.
- La procedencia, origen o fuente de los datos.
- Cuál es el destinatario de la información que le concierne, esto es, quién o quiénes utilizarán la referida información.
- El propósito, finalidad u objeto del almacenamiento, esto es, para qué se tratan los datos personales.
- La individualización de las personas u organismos a los cuales sus datos son transmitidos o comunicados regularmente. En este último caso surge un problema: qué se debe entender por "regularmente", la ley guarda silencio a este respecto. El Diccionario de la Lengua Española señala que significa comúnmente, ordinariamente, definición que no ayuda mucho. Creemos, que este vocablo se debe interpretar en el sentido de que deben tratarse de transmisiones que no se hayan efectuado por una sola vez y que revistan un cierto carácter de periodicidad.

Por último, en esta parte, hay que considerar el artículo 14 de la Ley, el cual tiene especial aplicación para el tratamiento de datos que efectúan organismos públicos, el cual indica: "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." Este artículo regula la figura de los bancos de datos compartidos por diversos órganos, basta en todo caso, para que se aplique la norma que los diversos organismos tengan acceso al banco de datos en cuestión. Se indica que el titular de los datos podrá ejercer el derecho de información respecto de cualquiera de ellos. Se hace hincapié, en que sólo se trata del derecho de información, el resto de los derechos deberá ejercerlos respecto del órgano a quien le compete las decisiones relacionadas con el tratamiento de los datos personales en cuestión.

---

obtener de él información sobre aquellos que le conciernen y que se encuentran incorporados en ella. CERDA, Alberto. op. cit. pág. 80.

2.7.2.2. El derecho de modificación.

Es la facultad de todo titular de datos para solicitar la rectificación de aquellos datos que le conciernen, cuando éstos sean erróneos, inexactos, equívocos o incompletos[324]. La Ley exige acá, un requisito que no se encuentra presente para el ejercicio de los otros derechos, cual es que se debe acreditar por parte del titular de los datos la "mala calidad" del dato que se reclama, lo que usualmente, se efectuará a través de documentos.

Ahora bien, entendemos según las definiciones dadas por el Diccionario de la Real Academia de la Lengua Española, por dato erróneo, el falso o equivocado, por dato inexacto, aquél falto de fidelidad[325], por dato equívoco, el que produce confusión o interpretaciones diversas y por último, por dato incompleto, aquél que le falta información.

En conclusión, se puede señalar que procederá la modificación de los datos cada vez que un dato no se corresponda a la realidad actual de la que da cuenta.

2.7.2.3. Derecho de cancelación o eliminación.

Es la facultad de todo titular de datos para exigir la destrucción de los datos almacenados, cualquiera fuere el procedimiento empleado para ello, cuando el almacenamiento de los datos carezca de fundamento legal o cuando estuvieren caducos.

El dato carecerá de fundamento legal cada vez que se efectúe un tratamiento de datos sin autorización legal o convencional[326]. De su parte, conforme el artículo 2 letra d) de la Ley, el dato deviene en caduco cuando:

---

[324] La voz "modificación" se emplea en forma genérica, para describir cualquier cambio en los datos almacenados que no importe eliminarlos. Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2114. 05 de agosto de 1998.

[325] A propósito de los datos erróneos o inexactos, Hernán Corral señala que "aunque la ley diferencie los vocablos, nos parecen que coinciden; lo erróneo es inexacto y viceversa". CORRAL, Hernán. op. cit. pág. 44.

[326] Para el legislador que los datos carezcan de fundamento legal comprende dos ideas distintas. La primera se refiere, en general, a aquellos datos personales que nunca pudieron haber estado en un banco de datos. La segunda, a los datos personales recogidos por una institución cuya finalidad es muy específica y esos datos no guardan relación con ella. Informe de la Comisión de Constitución,

- La ley así lo disponga.
- Por el cumplimiento de la condición señalada para su vigencia.
- Por la llegada del plazo señalado para su vigencia.
- Y, finalmente lo más importante, cuando se ha producido un cambio en las circunstancias o hechos que consigna, a menos que una norma expresa establezca lo contrario.

El artículo 12 inciso final de la ley, establece una regla muy importante para el caso de los datos cancelados o modificados, al señalar que: "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".

2.7.2.4. El derecho de bloqueo.

Es el que le corresponde a todo titular de datos para exigir la suspensión temporal de cualquiera de las operaciones del tratamiento de datos; este bloqueo procederá en todos aquellos casos en que la exactitud de los datos no pueda ser establecida o su vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.[327]

Si bien la Ley define el bloqueo de datos, en su artículo 2 letra b) como la supresión temporal de cualquiera de las operaciones del tratamiento de datos, lo cierto es que, en la práctica, el bloqueo de datos se traduce en la imposibilidad de comunicar el dato bloqueado a terceros.

Finalmente, se establece que se podrá pedir ya sea la cancelación o el bloqueo de los datos, según corresponda, en los casos de las listas de datos que se utilizan para comunicaciones comerciales (marketing directo) y se ejerce el derecho para el caso que no se desee continuar

---

Legislación y Justicia recaído en el proyecto de ley sobre protección a la vida privada. Cámara de Diputados. Segundo Trámite. Sesión 3, pág. 167. 04 de junio de 1996.

[327] Es el típico caso de los datos que son objeto de un litigio.

figurando en el registro respectivo, ya sea en forma temporal o definitiva, y finalmente cada vez que se hayan proporcionado los datos en forma voluntaria.[328]

2.7.2.5. Otros derechos

Además de estos cuatro derechos troncales, la ley señala tres más, que es de pertinencia mencionar aquí:

i) Obligación de comunicación a terceros: Si se han modificado o cancelado determinados datos personales que han sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada (la de modificación o cancelación[329]). 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[330].

ii) Derecho de oposición: El artículo 3 inciso final de la ley, señala que "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión". Pensamos que esta oposición puede ejercerse en cualquier etapa del tratamiento de los datos, ya sea en su recogida, almacenamiento, transferencia, etc.[331]

---

[328] Art. 12 inciso 4° Ley 19.628: "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". Esta norma se discutió en el Senado, quedando constancia de que se complementó también la posibilidad de exigir que se supriman los datos cuando se hayan proporcionado voluntariamente con la de pedir que se bloqueen. Estas dos opciones las tendrá el titular de los datos también cuando éstos se usen para comunicaciones comerciales, lo que parece lógico, sobre todo si se considera que, en el artículo 4º que se propondrá a la Comisión Mixta, se admite que la actividad comercial denominada comúnmente "marketing directo" no necesita autorización del titular de los datos para someterlos a tratamiento, siempre que ellos provengan o se recolecten de fuentes accesibles al público. Diario Sesiones del Senado. Sesión 18, tomo 2114, pág. 2094. 05 de agosto de 1998.

[329] Se llama la atención con respecto a la circunstancia de que este derecho no opera en hipótesis de bloqueo de datos.

[330] Artículo 12 inc. 5° Ley 19.628. "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."

[331] Esta norma, a falta de una que regule la materia en forma expresa, puede servir de base para oponerse ya sea en sede extrajudicial como en sede judicial, al denominado *spam*, o correo electrónico no deseado, ya que en él se utilizan datos personales justamente con fines de publicidad.

iii) Derecho de copia: Además, se impone en nuestra ley, la obligación al titular de los bancos de datos de entregar, a solicitud del titular, copia del registro alterado en la parte pertinente, este es el denominado "derecho de copia". Ahora bien, este derecho a copia gratuita se encuentra limitado, ya que se señala que cada vez que se modifiquen o eliminen datos podrá ejercerse este derecho gratuitamente, pero siempre que hayan transcurrido seis meses desde la última vez que se hizo uso de este derecho. Además, este derecho, conforme al inciso 4 del artículo 12 de la Ley, deberá ejercerse personalmente[332].

2.7.2.6. Límites al ejercicio de estos derechos.

La Ley limita en su artículo 15 la posibilidad de ejercicio de estos derechos por parte del titular de los datos, en cuatro hipótesis[333]:

[332] La inclusión de estas limitaciones (plazo de seis meses y ejercicio personal del derecho de copia) fueron incluidos en el proyecto por la Comisión Mixta por una sugerencia que recibió de Dicom en la que esta empresa solicitaba que se restableciese el lapso mínimo de doce meses para hacer uso del derecho de acceso, como había contemplado la Honorable Cámara de Diputados. Hizo presente esa firma que la ausencia de todo plazo podría prestarse para abusos, a través de empresas que se dedicasen a obtener mandatos de los titulares de datos para ese objetivo. Informó que, en promedio, las personas naturales que solicitan informes comerciales lo hacen en un 50% respecto de ellas mismos y en un 50% respecto de terceros. Las razones que originan esas solicitudes de informes corresponden a transacciones comerciales, como presentación de ellos para una operación crediticia, participación en licitaciones públicas o privadas, pago de deudas en mora, postulaciones a subsidios habitacionales y otros fines, todos en su directo beneficio. De ahí que no limitar el derecho de acceso gratuito a la información iría en evidente perjuicio patrimonial del prestador del servicio. Por último, añadió que la legislación internacional que contempla el derecho de acceso gratuito a la información lo limita a una vez al año, como ocurre en Estados Unidos y en España. Estas consideraciones fueron atendidas por la Comisión Mixta, la que resolvió, por una parte, impedir el otorgamiento de mandato para estos efectos, disponiendo que el derecho a obtener copia gratuita sólo puede ejercerse personalmente. Por otro lado, procurando conciliar los intereses del titular de los datos con los del responsable del banco de datos, razonó que, informada una persona de sus datos personales conforme figuran en el banco, sólo resulta razonable que pida una copia del registro actualizado si han mediado nuevas modificaciones o eliminaciones de datos. Para ello, creyó que un lapso de seis meses entre cada oportunidad en que desee hacer uso del derecho de acceso gratuito resulta prudente, ya que, además, lo podrá hacer en cualquier tiempo pagando el costo del servicio. Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 116. 02 de junio de 1999. Para un comentario doctrinario de estas limitaciones ver PALAZZI, Pablo. op. cit. pág. 183.

[333] Entendemos a partir del contenido de las excepciones, como asimismo, de la discusión que se produjo durante la tramitación del proyecto de ley, que los únicos legitimados para invocar estas causales como motivo de rechazo del ejercicio de los derechos por parte del titular de los datos, son los organismos públicos respectivos.
En la tramitación del proyecto de ley el Ejecutivo sugirió que la ley encomendase a su Excelencia el Presidente de la República que, mediante decreto supremo, individualizare los organismos públicos a los que no se aplicarán las normas de este título. La Comisión Mixta estuvo en desacuerdo con la idea de facultar a su Excelencia el Presidente de la República para excluir a determinados organismos públicos de disposiciones centrales de esta iniciativa de ley, como son las que desarrolla su Título II, porque ello significaría, en la práctica, instaurar dos regímenes paralelos en materia de protección de datos personales, uno de ellos particularmente variable por simple decreto supremo, con la consiguiente restricción en los derechos de los titulares de datos. Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 120. 02 de junio de 1999.

i) Cuando impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido. Por ejemplo, si un contribuyente solicita datos personales de carácter tributario del año en curso al SII.

Esta excepción fue discutida en el Senado, debido a la intervención efectuada por el Ejecutivo que informó que el Ministro de Hacienda y el señor Director del Servicio de Impuestos Internos habían pedido, derechamente, que se estableciera que estas normas no se aplicaran al Servicio de Impuestos Internos. Lo anterior, debido a que al entender del Director del SII, la obligación de suministrar los datos a las personas a los cuales pertenecen, con indicación de la fuente de la que se obtuvieron y eventuales destinatarios, el propósito del almacenamiento e individualización de personas y organismos a los cuales son transmitidos regularmente, hará ilusorios e ineficaces los procedimientos y estrategias del Servicio destinados a obtener que los contribuyentes declaren fielmente sus ingresos y gastos, para determinar, en cada caso, las bases imponibles con sujeción estricta a valores reales, por cuanto resulta obvio que aquéllos, al saber exactamente los datos registrados a su respecto en el Servicio, ajustarán sus declaraciones de impuestos sólo a estos datos, excluyendo del escrutinio fiscal cualquier otro ingreso no considerado en dichos antecedentes. A lo anterior, agrega que el Servicio se vería enfrentado a una gran demanda de parte de los contribuyentes para obtener los datos que a su respecto registra la administración tributaria, con la finalidad ya señalada, lo que traerá el consiguiente costo administrativo y desvío del objetivo institucional, cual es la fiscalización tributaria. La Comisión Mixta frente a esta inquietud, tuvo en cuenta que está referida particularmente a datos que le solicite el propio contribuyente sobre actos realizados durante el mismo período tributario, ya que, si recaen sobre declaraciones ya efectuadas, desaparece la razón de ser de la objeción de ese Servicio. Otra forma en que se podría afectar la labor fiscalizadora sería en aquellos casos en que un contribuyente está siendo objeto de investigación y requiere los datos que el Servicio ha recopilado a su respecto. Por lo mismo, juzgó la Comisión Mixta que, en la especie, el interés social estará bien cautelado si se restringen los derechos del Título II de la Ley, sólo a aquellas situaciones en que se impide o entorpece el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, y no en cualquier otro caso, ya que debe reconocerse a los titulares de los datos herramientas que les permitan

acceder a información sobre ellos, con el objeto de poder instar por la corrección de eventuales errores o equivocaciones o, en general, para conocer la información que obre a su respecto[334].

ii) Afecte el derecho de reserva o secreto establecido en disposiciones legales o reglamentarias. Por ejemplo, si se trata de datos personales que constan en expedientes judiciales que revisten el carácter de secreto según la ley, como en el caso de las adopciones o juicios de menores, o el denominado secreto bancario.

iii) Afectación de la seguridad de la nación o el interés nacional. Con respecto a este punto podemos señalar que se trata de conceptos jurídicos indeterminados, por lo que serán los Tribunales de Justicia los llamados a determinar si se dieron los presupuestos de hecho necesarios para considerar que la solicitud en cuestión por parte del titular de los datos pudo haber afectado la seguridad de la nación o el interés nacional.

Respecto a esta excepción, durante la tramitación del proyecto el Ejecutivo estimó que las circunstancias que habilitan a los organismos públicos para negarse a proporcionar información, o a modificar, cancelar o bloquear datos personales no estaban adecuadamente configuradas, por ejemplo, al emplear el concepto de "seguridad pública", que tiene un alcance más restringido que el de "seguridad de la Nación" o el de "interés nacional", o al exigir que se trate de materias cubiertas por el secreto "conforme con la ley", lo que se prestaría a dudas con todas las materias cuya calificación de secreta o reservada emana de normas reglamentarias. En cuanto a estas observaciones la Comisión Mixta las salvó empleando los conceptos de "afectar la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional"[335].

iv) Datos almacenados por mandato legal, salvo que la propia ley lo autorice. Se trata acá, de registros o bancos de datos creados por ley. En todo caso, la limitación no se hace extensiva al derecho de información.

[334] Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 120-121. 02 de junio de 1999.
[335] Ibídem.

2.7.2.7. Derecho a accionar (Hábeas Data)

2.7.2.7.1. Generalidades

Consideramos, por último, el derecho que tiene todo titular de datos de accionar con el objeto de obtener amparo judicial frente a eventuales tratamientos ilegítimos de los datos personales que le conciernes denominado por la doctrina como hábeas data[336].

En nuestro país el control de la legalidad en el tratamiento de datos, se efectúa *ex post* por parte del titular de los datos ejerciendo los derechos que le concede la ley ante los responsables de los bancos de datos ya sean estos privados o públicos, o bien, ante los Tribunales de Justicia mediante el ejercicio por parte del afectado de la acción de hábeas data que ha sido consagrada con rango legal en el artículo 16 de la Ley de Protección a la Vida Privada[337], a diferencia de la generalidad de los ordenamientos a nivel latinoamericano que tienen legislaciones protectoras de datos en donde se recibe reconocimiento constitucional a esta acción, como por ejemplo, Colombia, Perú, Paraguay, Argentina.

De esta manera, el hábeas data se configura en nuestro ordenamiento como el instrumento a través del cual, los titulares de datos pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que le concierne por parte del responsable del registro o banco de datos.

[336] El concepto de hábeas data, tiene dos acepciones, a veces se lo trata como derecho constitucional o legal de las personas con raíces en el derecho a la intimidad, frente al tratamiento automatizado de sus datos; en otras, se atiende a su función como garantía o proceso jurisdiccional que tiene por objeto amparar los derechos del titular de los datos ante tratamientos indebidos o ilegítimos de la información de naturaleza personal que le concierne. En nuestro caso, hablamos de hábeas data en esta segunda acepción. Para una muy buena conceptualización del concepto ver GOZAINI, Osvaldo. 2001. Hábeas data. Protección de datos personales. Doctrina y jurisprudencia. Buenos Aires, Rubinzal-Culzoni. 526p.

[337] Sin embargo, en la práctica los titulares de datos para proteger sus derechos han utilizado la interposición de otras acciones jurisdiccionales como por ejemplo: el recurso de protección, invocando como conculcados el derecho a la honra y a la vida privada, el derecho de propiedad (esto por la conocida propietarización de los derechos), o bien, el derecho al libre desarrollo de actividad económica. También, aun cuando con menor frecuencia, se han interpuesto recursos de amparo económico, por vulnerar la garantía constitucional que asegura el libre desarrollo de la actividad económica. Y finalmente, también se han interpuesto demandas de indemnización de perjuicios por los daños causados por el tratamiento indebido de los datos. Para un completísimo estudio empírico del tema ver proyecto de investigación "Intimidad y nuevas tecnologías. Análisis de la tutela efectiva a los derechos de los titulares de datos personales en Chile". Concurso de Ciencias Sociales, Humanidades y Educación DID 2002.

2.7.2.7.2. Causales o presupuestos fácticos de procedencia del hábeas data[338].

i) Si el responsable del registro o banco de datos no se pronunciare sobre una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales dentro de dos días hábiles. (Art. 16 inc. 1°).

ii) Si el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por una causa distinta de la seguridad de la Nación o el interés nacional. (Art. 16 inc. 1°).

iii) Si el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por motivos de seguridad de la Nación o el interés nacional. (Art. 16 inc. 3°).

iv) Con la modificación introducida por la Ley 19.812, también se puede reclamar a través de este procedimiento por infracción a los artículos 17 y 18 de la Ley 19.628, que regulan la forma y los plazos en que pueden comunicarse a terceros datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial. (Art. 16 inc. 5°).

v) Infracciones no contempladas en los artículos 16 y 19. (Art. 23 inc. 2°).

2.7.2.7.3. Tribunal competente.

La ley entrega la competencia al Juez Civil de Turno correspondiente del domicilio del responsable del banco de datos de que se trate, o sea, sigue la regla general en materia de competencia relativa existente en nuestro ordenamiento jurídico: el domicilio del demandado.[339]

[338] Esta clasificación se efectúa sobre la base de distintos presupuestos o causales que se encuentran dispersas en distintos artículos de la Ley, y que han sido ordenados de esta manera para una mayor claridad al lector.

[339] El punto fue debatido en el Parlamento; la otra opción en relación al Juzgado competente para conocer del hábeas data, fue otorgar competencia al Juez del domicilio del afectado, o bien, entregar la posibilidad de elegir entre éste y el del domicilio del demandado, pues optar por la regla general, implicaría dificultar el ejercicio del derecho, ya que gran parte de los domicilios de los responsables de bancos de datos se encuentran en la Región Metropolitana. Finalmente, se optó por seguir las reglas generales. Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 106. 02 de junio de 1999.

2.7.2.7.4 Legitimación activa y pasiva.

El legitimado para interponer el reclamo es el afectado, esto es, el titular de datos que ha visto vulnerados sus derechos reconocidos en la Ley, con el objeto de solicitar amparo de ellos al Tribunal.

Luego, el legitimado pasivo de este reclamo es el responsable del banco de datos, ya sea particular u organismo público. Se establece una regla especial en el artículo 14 de la ley que señala que en el evento en que los datos personales estén en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos, de esta manera en el evento de que así lo hiciese, podrán ser sujetos pasivos de la acción dos ó más organismos públicos.

2.7.2.4.5. Procedimiento

Ya establecidas las causales por las que procede el recurso, cuál es el tribunal competente, quién puede interponerlo y en contra de quién, debemos proceder ahora, a analizar el procedimiento de reclamo. Dado que la ley establece tres tipos de procedimientos, según sean las causales invocadas, para efectuar un análisis de ellos lo correcto metodológicamente hablando es estudiar tales procedimientos desde el enfoque de las causales esgrimidas para la interposición del hábeas data.

i) Procedimiento general de reclamo.

Distingue el artículo 16 de la Ley, que es el que establece el procedimiento de reclamación, dos hipótesis y dos procedimientos distintos, según sea la causal que dio origen al reclamo. El primero de ellos se aplica a las causales que siguen:

- Si se trata de la falta de pronunciamiento por parte del responsable del banco de datos dentro de los dos días hábiles siguientes al requerimiento presentado por el titular de los

datos, o bien denegase la información por una causal distinta de la seguridad de la nación o el interés nacional.

- Infracción a los artículos 17 y 18 de la Ley 19.628, se procede de la siguiente manera:

a) Se debe presentar una reclamación, ante el Tribunal Civil de Turno, esta reclamación debe contener, según la Ley, a los menos:

- Indicación clara de la infracción cometida y los hechos que la configuran.
- Acompañar los medios de prueba que los acrediten, en su caso.

b) Este reclamo se notifica por cédula en el domicilio del responsable del banco de datos correspondiente.

c) El responsable del banco de datos deberá en al contestar al traslado dentro de quinto día hábil, señalando:

- Sus descargos.
- Adjuntar los medios de prueba que acrediten los hechos en que funda estos descargos. En el evento de que no disponga de los medios de prueba deberá señalarlo así, ahora bien, si ofrece prueba el tribunal fijará una audiencia, para dentro de quinto día hábil a fin de recibir la prueba ofrecida y no acompañada.

Esta facultad que se le entrega al demandado, facultad de la cual está desprovisto el reclamante o afectado, constituye uno de los puntos más criticables de este procedimiento pues vulnera uno de los principios fundamentales de todo procedimiento cual es el de la bilateralidad de la audiencia, al dejar en manos del responsable del banco de datos, la posibilidad de que exista una audiencia de prueba, ya que si no ofrece prueba, no existirá tal audiencia.

d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo para presentar descargos, sea hayan o no presentado descargos. Ahora bien, si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) La sentencia definitiva se notifica por cédula y es 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.

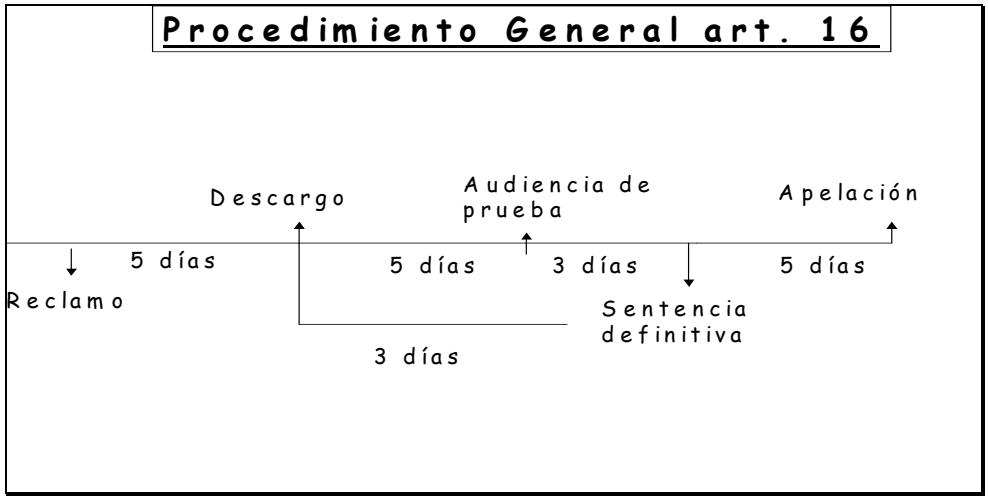
f) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. En todo caso, si la Corte lo estima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

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

h) 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

Cuadro Nº 1

Procedimiento General de Hábeas Data del artículo 16 de la Ley 19.628



ii) Procedimiento especial de reclamo.

A este segundo procedimiento lo he denominado especial, frente al general que ya revisáramos. Es especial pues sólo se aplica en el evento que la causal invocada para denegar la solicitud del requeriente por parte del responsable del banco de datos sea la seguridad de la Nación o el interés nacional, y especial, en segundo lugar, porque sólo puede dirigirse en contra de organismos públicos, ya que ellos son los únicos legitimados para invocar la causal indicada. Afirmo esto, pues, no cabe que un ente privado fundamente su negativa a acceder a una determinada solicitud de un titular en causales que dada su entidad, sólo pueden ser invocadas por el Estado y sus organismos, y también por que así se concluye de la historia fidedigna de la ley, cuando por ejemplo se señala: "...las circunstancias que habilitan a los organismos públicos para negarse a proporcionar información, o a modificar, cancelar o bloquear datos personales, no están adecuadamente configuradas, por ejemplo, el emplear el concepto de "seguridad pública", que tiene un alcance más restringido que el de "seguridad de la nación" o el de "interés nacional"[340].

En este caso, las reglas procedimentales son las que siguen, según lo estatuido en la propia ley:

a) 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. La competencia radica en nuestro más alto Tribunal de Justicia, dada la entidad de la causal invocada para el rechazo de la solicitud, y dado también, que una de las partes será un órgano del Estado.

b) 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 requeriente.

c) La sala de la Corte Suprema que conozca la reclamación, 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. El Presidente del Tribunal dispondrá que la audiencia no sea pública.[341]

iii) Procedimiento residual.

Finalmente, si estamos en presencia de una cualquier otra infracción que no sea de las contempladas en el artículo 16 y 19, se aplica el procedimiento sumario, según lo establecido en el artículo 23 de la Ley.[342] Por ejemplo, si el órgano público trata datos fuera del ámbito de su competencia, o si el responsable de datos no cumple con la obligación de avisar a terceros que los datos han sido modificados o eliminados, etc.

2.7.2.4.6. Sanciones

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 1 a 10 unidades tributarias mensuales o de 10 a 50 unidades tributarias mensuales, si se tratare de una infracción a lo dispuesto a los artículos 17 y 18 de la Ley. Esta última multa fue agregada por la Ley 19.812, y, como ya señaláramos, se refiere al caso de infracciones a la ley en la comunicación de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial.

Finalmente, indica la Ley, que 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 2 a 50 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.

---

[340] Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 120. 02 de junio de 1999

[341] Como es dable observar, este procedimiento reviste caracteres de secreto, debido a las posibles implicancias, nuevamente, de la causal invocada.

[342] Artículo 23 inciso 2° Ley 19.628 "En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de perjuicios, se sujetarán al procedimiento sumario".

8. Responsabilidad

Revisaremos las reglas de responsabilidad establecidas en la Ley, conforme a los siguientes elementos: Naturaleza de la responsabilidad, imputabilidad, daños, acción de indemnización de perjuicios, y la responsabilidad en el caso de tratamiento por mandato.

2.8.1. Naturaleza de la responsabilidad

El artículo 23 de la Ley indica que el responsable del tratamiento de datos, ya sea un particular o un organismo público, debe indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos[343]. Se trata de una hipótesis de responsabilidad civil extracontractual por culpa.

Creemos que la ley regula un supuesto de responsabilidad por culpa y no objetiva por las siguientes razones: al hablar la ley de "tratamiento indebido de los datos", de "debida diligencia", se concluye que se exige culpa o negligencia en el actuar del responsable de datos; la historia de la ley indica que se optó por este tipo de responsabilidad al estimar la Comisión Mixta[344] apropiada la sugerencia de ACTI de precisar que la indemnización de perjuicios que se consagra procederá cuando exista un tratamiento "indebido" de los datos de una persona, ya que ello despeja cualquier duda acerca de la aplicación de las reglas generales de responsabilidad extracontractual consagradas en el Código Civil; y por último, porque el régimen común de responsabilidad extracontractual establecido en nuestro ordenamiento es el basado en la culpa o negligencia, de manera que desechamos el entender que la ley establece una hipótesis de responsabilidad de tipo objetivo o estricto [345].

---

[343] El concepto "tratamiento indebido de datos" abarca, según el proyecto de modificación de la Ley 19.628 que se tramita actualmente en el Parlamento, cualquier conculcación al legítimo ejercicio de los derechos garantizados por la Constitución o las leyes, que se produzca como consecuencia del tratamiento de datos, aun cuando haya autorización por parte de su titular, y el tratamiento se efectúe en las hipótesis autorizadas por la Ley 19.628 u otras disposiciones legales lo autoricen. Boletín: N° 3095-07 "Proyecto de ley que modifica la ley N° 19.628, sobre protección de datos de carácter personal para introducir el concepto de uso indebido o abusivo de datos", ingresado con fecha de 15 de Octubre de 2002.

[344] Diario Sesiones del Senado. Sesión 2, tomo 99, pág. 136. 02 de junio de 1999

[345] Comparten esta interpretación CORRAL, Hernán. op. cit. pág. 55 y GONZÁLEZ, Francisco. 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. En

2.8.2. Imputabilidad.

Respecto a la imputabilidad, a lo largo de la ley es posible encontrar una serie de normas que establecen los deberes del sujeto responsable del registro o banco de datos personales[346].

a) Obligación general de cuidado

El artículo 11 indica que el responsable de los registros o bancos donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. Este artículo obliga al organismo público o privado a indemnizar el daño que causare por el procesamiento, utilización y divulgación de los datos personales, cuando no se hubieren adoptado todos los resguardos técnicos necesarios para evitar un error en el almacenamiento de los mismos o hubiere habido negligencia en su manejo[347]. La norma en comento fue incluida en el tercer trámite constitucional debido a que la Comisión estimó adecuado que, "sin perjuicio de que el proyecto de ley regule más adelante la responsabilidad civil del responsable del banco de datos personales, exista una norma sustantiva que ordene emplear la debida diligencia en la utilización de los datos. Esa diligencia será la que corresponda de acuerdo a las reglas generales del Código Civil"[348], es decir, se extiende hasta la culpa leve."[349]

b) Obligación de secreto

El artículo 7 de la ley consagra la obligación de secreto que pesa sobre las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, cuando los referidos datos personales provengan o hayan sido recolectados de fuentes no

---

contrario, CERDA, Alberto. op. cit., pág. 39. "El legislador ha establecido un sistema de responsabilidad objetivo en la materia, que prescinde de la concurrencia de un elemento subjetivo en el agente y al cual basta la constatación de que el tratamiento sea ha verificado indebidamente. Por lo demás, tal sistema es el que mejor se aviene con el propósito de salvaguardar los derechos del titular frente a los riesgos que importa el tratamiento de sus datos mediante el empleo de las nuevas tecnologías".

[346] VIAL, Felipe. op. cit. pág. 35.

[347] Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2110. 05 de agosto de 1998.

[348] Ibídem.

[349] VIAL, Felipe. op. cit. pág. 36.

accesibles al público, como asimismo, sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo. Llama la atención de esta norma, que establezca el deber de secreto respecto a las personas que trabajan en el tratamiento de datos, y que nada diga en forma directa sobre el establecimiento de este deber respecto del responsable del banco de datos. En todo caso, en la práctica si se produce la vulneración a este deber de secreto por parte de alguno de los que trabajan en el tratamiento de datos personales, se puede configurar una hipótesis de responsabilidad por el hecho ajeno (de los dependientes) para el responsable del banco de datos respectivo.

c) Obligación de mantener calidad de los datos

El principio de calidad de los datos, se ve reflejado en dos artículos que establecen la obligación para el responsable del banco de datos de mantener dicha calidad. Así, el inciso final del artículo 6 indica que "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"[350] y el inciso segundo del artículo 9 que señala que "En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos."

d) Obligación de tratamiento conforme al fin

El articulo 9 de la Ley señala en su inciso primero que "Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público". La excepción al principio de finalidad cuando los datos provienen o se han recolectado de fuentes accesibles al público, ha sido duramente criticada por la doctrina nacional, Alberto Cerda[351] a este respecto indica que "no deja de llamar a reparos tal excepción, cuyo alcance queda contradicho por el propio tenor del

[350] Respecto de esta obligación resulta clarificador reproducir lo señalado en la tramitación del proyecto de ley: "Por último, si bien estuvo de acuerdo en que la eliminación, modificación o bloqueo de los datos son facultades del titular, como se reconoce más adelante, no le pareció consecuente con el propósito de esta ley premiar la actuación u omisión dolosa o negligente del responsable del banco de datos que no adopte las medidas pertinentes para reparar situaciones que afecten al titular, por lo que resolvió imponerle un deber de actuación. Para ello, hizo recaer en el responsable del banco de datos personales la obligación de eliminación, modificación o bloqueo de los datos, según corresponda, aunque no medie requerimiento del titular de los mismos". Diario Sesiones del Senado. Sesión 18, tomo 2034, pág. 2117. 05 de agosto de 1998.
[351] CERDA, Alberto. op. cit. pág. 73.

artículo 4 de la Ley, que, como hemos visto más arriba, al admitir el tratamiento de datos personales sin el consentimiento del titular, contempla la hipótesis de aquellos provenientes de tales fuentes, si bien circunscribiendo su finalidad a tres eventos".

Concluimos en esta parte señalando que el responsable del banco de datos personales debe cumplir con las obligaciones mencionadas y, en general con todos aquellas normas que le impongan un determinado deber de conducta en relación al tratamiento, como asimismo, debe respetar los derechos del titular de los datos, tanto se trate de sus derechos fundamentales como de los derechos subjetivos que le reconoce la ley.

2.8.3. Daños

El ya mencionado artículo 23 establece que 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 su caso, lo ordenado por el tribunal.

Se optó por mencionar expresamente la procedencia del daño moral debido a que la redacción del precepto en su moción original sugería que habría lugar solamente a la reparación de los perjuicios morales, excluyéndose los daños patrimoniales, lo que no es propio. Por lo que la Comisión convino en dar cabida expresamente a la reparación tanto de los daños morales como patrimoniales. Del mismo modo, la Comisión adecuó la redacción, a fin de clarificar la aplicación de las reglas probatorias generales, en el sentido de que la indemnización procede en la medida que haya algún daño efectivo, esto es, se acrediten los perjuicios[352].

2.8.4 Acción de indemnización de perjuicios.

El artículo 23 de la Ley sienta como principio general que la obligación de indemnizar, que recae sobre el responsable del banco de datos personales, no obsta a su deber de eliminar, modificar o bloquear los datos, según corresponda. De su parte, la acción de indemnización de perjuicios respectiva puede ser conocida a través de tres procedimientos, veamos:

1.- La regla general es que lo sea en forma conjunta con el procedimiento de reclamo o hábeas data, ya que el artículo 23 de la Ley permite que se interponga la acción indemnizatoria en forma conjunta con la reclamación destinada a establecer la infracción (la del artículo 16), sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil, esto es, que en el evento en que no se discuta sobre el monto de los perjuicios en el procedimiento de reclamo, se permite la reserva del derecho de discutir esta cuestión en la ejecución del fallo o en otro juicio diverso.

2.- La segunda opción es interponer la acción de indemnización de perjuicios en procedimiento ordinario, según las reglas procedimentales generales.

3.- Finalmente en juicio sumario, ya que la ley establece una regla residual que permite que todas las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujeten al procedimiento sumario.

Se indican, asimismo, en el artículo 23 tres reglas que el juez debe seguir en el conocimiento de las acciones de reclamo y/o de indemnización de perjuicios que conozca, entendiendo que estas reglas se aplican a todos los procedimientos regulados en Ley 19.628, a saber:

a) El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece.

b) La prueba se apreciará en conciencia por el juez.

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

---

[352] Diario Sesiones del Senado. Sesión 63, tomo 7383, pág. 7503. 05 de enero de 1993.

2.8.5. La responsabilidad en el caso de tratamiento por mandato

Resulta interesante revisar la responsabilidad en caso de tratamiento indebido de datos cuando éste es efectuado por un tercero a través de un mandato. Recordemos que la propia Ley regula en su artículo 8 este tipo de tratamiento. Indica la norma citada que 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.

Sin embargo, la Ley no resuelve el tema de la responsabilidad en el tratamiento de datos efectuado por mandato. No obstante ello, podemos señalar que el mandatario deberá responder por los actos que generen algún tipo de daño a un titular de datos, cuando tales actos sean realizados fuera de las condiciones de la utilización de los datos que han sido determinadas por el mandante y que la ley hace obligatorias de mencionar por escrito. Ahora bien, si el mandato se ejecuta dentro de las atribuciones y funciones expresamente pactadas, creemos que será el responsable del tratamiento quien tendrá la responsabilidad última ya que es él, quien toma las decisiones relacionadas con el tratamiento de datos, no perdiendo la calidad de tal a consecuencia del mandato.

CAPITULO TERCERO

CARACTERIZACIÓN DEL MERCADO DE DATOS PERSONALES EN CHILE

3.1.- Consideraciones previas

Ya en el año 1993 al presentarse el proyecto de ley sobre protección a la vida privada, se reconocía: "Todos los detalles de nuestra vida privada se encuentran en la actualidad archivados en más de algún computador, engrosando voluminosos bancos de datos. Nombre, edad, estado civil, direcciones particular y profesional; integrantes del grupo familiar, sus identidades y colegios donde estudian; enfermedades que han tenido los componentes de la familia, actividades deportivas, culturales y recreativas habituales; ingresos económicos del grupo familiar, cuentas de crédito, corrientes y de ahorro; seguros de vida y de accidentes contratados; patrimonio en bienes raíces y bienes muebles, etcétera. Dichos antecedentes son manejados en la actualidad por los bancos, compañías de seguros, administradoras de fondos de pensiones, instituciones de salud provisional, empleadores y casas comerciales, en términos tales que prácticamente los detalles más importantes de nuestras respectivas personas y familias están expuestos hoy a su manipulación por parte de terceros, situación que debe ser regulada por la ley"[353].

Es claro que nuestro país no se encuentra ajeno a la utilización de las herramientas tecnológicas con el fin de recolectar, almacenar, procesar, cruzar y comunicar datos personales. Hoy en día y más que nunca el mercado de datos personales presenta una multiplicidad de actores y constituye una parte importante de la economía, tanto por la cantidad de transacciones que se generan como asimismo por la relevancia que en ella tiene el contar con determinada información de naturaleza personal[354].

[353] Diario Sesiones del Senado. Sesión 20, tomo 2890, pág. 3081. 05 de enero de 1993.
[354] Rony Jara reconoce lo señalado al indica que "...este trabajo aborda un tema que en esta sociedad de la información y economía de mercado en que vivimos ha adquirido una importancia creciente: el tratamiento de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial...". JARA, Rony. op.cit. pág. 61. Aun cuando este autor restringe su sentencia a los

Son varios y por distintas razones los actores que se ven involucrados en el mercado de datos personales[355]. Intentamos a continuación una clasificación de ellos:

a) fuentes primarias de información personal, esto es, las personas o entidades que entregan al mercado en forma directa datos personales, como por ejemplo: empresas acreedoras, organismos públicos, notarías, casas comerciales, instituciones financieras, registros públicos, Internet, prestadores de salud, y por último, los propios titulares de datos; b) fuentes secundarias de información personal, esto es, aquellos que distribuyen la referida información, comunicándola a terceros, generalmente en forma onerosa, y que se encuentran representados por las empresas que se dedican en forma exclusiva a distribuir datos como por ejemplo Dicom-Equifax y por aquellos que aun cuando la distribución de datos personales no constituye su giro principal, eventualmente sí distribuyen o comunican datos, como por ejemplo, el Servicio de Registro Civil e Identificación; c) usuarios finales de datos personales, son aquellos que buscan y adquieren la información personal para uso propio y que pueden ser personas naturales o jurídicas.

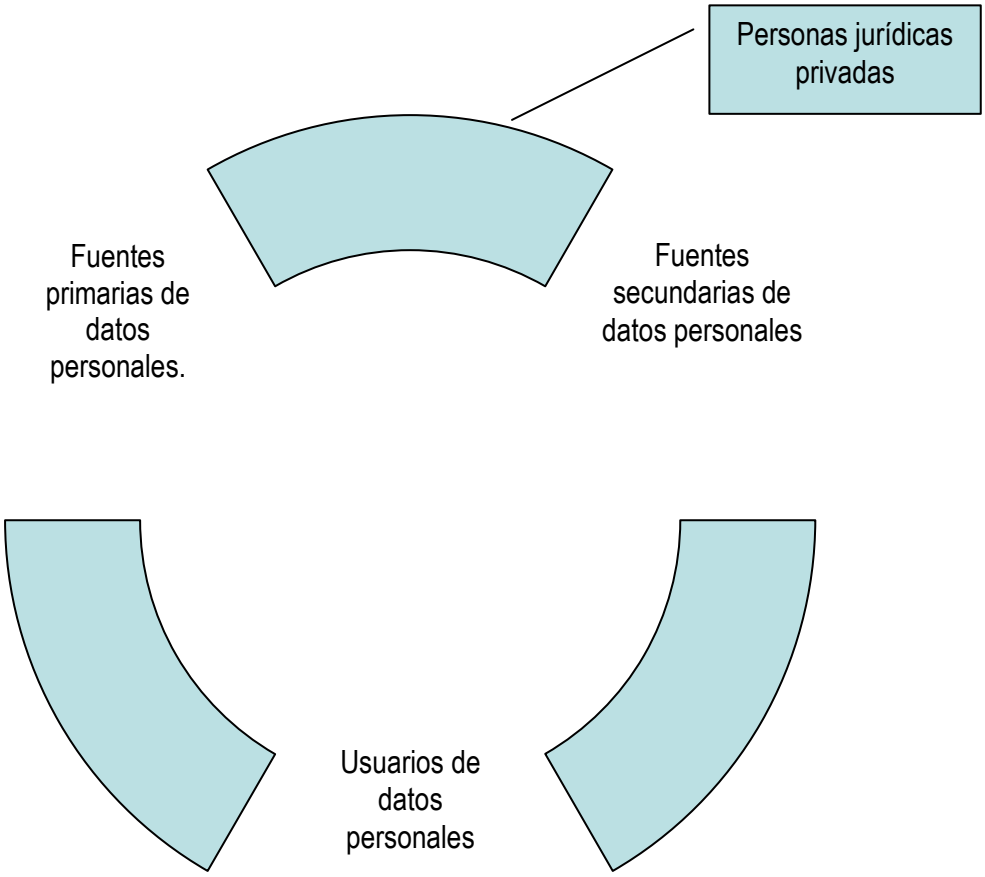
Un ejemplo concreto de la cadena podría ser el siguiente: una notaría (fuente primaria de datos personales) entrega información sobre cheques protestados a la Cámara de Comercio de Santiago que administra el Boletín Comercial, el que distribuye la información (fuente secundaria de datos personales) a quienes se lo soliciten (usuarios finales). En todo caso, puede ocurrir que no todos los eslabones de la cadena se encuentren presentes en una determinada transacción, ya que es posible que el usuario final pueda ir directamente a la fuente primaria en busca de la información que necesita, sin que en este caso tenga presencia la fuente secundaria de información. Asimismo, cabe hacer presente que se encuentra fuera de esta cadena por no poder distribuir los datos, las personas jurídicas privadas que tratan datos personales para el beneficio propio de ellas o de sus afiliados, hipótesis regulada en el inciso final de la Ley 19.628.

---

denominados en esta tesis datos patrimoniales negativos, creemos que cabe aplicarla a todos los tipos de datos personales que se transan en el mercado.

[355] Rodolfo Herrera se refiere a algunos de estos actores, "...la recepción no solicitada de correos electrónicos publicitarios, conocida como *spam*, o la actividad que realiza DICOM con las bases de datos de solvencia patrimonial y crédito, son sólo la punta del *iceberg*. Un aspecto de mucho más cuidado se observa, por ejemplo, en el caso del Estado como uno de los agentes potencialmente más peligrosos para los derechos fundamentales de los ciudadanos en la medida en que trate ilegítimamente sus datos personales". HERRERA, Rodolfo. La protección de datos personales como garantía básica de los derechos fundamentales. Revista de Derecho Público, de la Agrupación de Abogados de la Contraloría General de la República, Año Nº 2 (5). pág. 3.

Cuadro Nº 2



Por último, hemos de señalar que ha efectos de caracterizar el mercado de datos personales en nuestro ámbito, se ha dividido este mercado en diferentes tipos, según la naturaleza preeminente de la información o dato personal de que se trata, intentando responder a las siguientes preguntas: ¿quiénes actúan en este mercado?, ¿cuál es la fuente de los datos personales que tratan?, ¿qué tipo de datos tratan?, ¿comunican esos datos a terceros?, etc.

3.2. Mercado de datos patrimoniales

A estos efectos entenderemos como datos patrimoniales a aquellos que son de naturaleza económica, financiera, bancaria o comercial, es decir, utilizaremos el mismo lenguaje de la Ley 19.628 en su artículo 4 inciso 5, de manera que se comprenden tanto aquellos datos

patrimoniales negativos como positivos. Los principales actores de este mercado son Dicom S.A., la Cámara de Comercio de Santiago A.G (INFOCOM; databusiness, datarent y Boletín Comercial), la asociación de bancos e instituciones financieras (SINACOFI) y Servicios Integrados de Información S.A. (SIISA).

Dicom/Equifax, filial de la empresa norteamericana Equifax Inc., es la más grande y conocida de las empresas que se dedican a tratar datos personales patrimoniales en nuestro país. Opera en Chile desde hace 25 años aproximadamente y maneja el 70% del mercado de clientes de registros comerciales[356]. Las fuentes de información utilizadas por Dicom, son de una parte INFOCOM, que es una base de datos de la Cámara de Comercio de Santiago, que contiene todas las morosidades de las siete más grandes casas comerciales de Chile y del Boletín Comercial, también manejado por la señalada Cámara. Para obtener dicha información, las morosidades contenidas en INFOCOM y en el Boletín Comercial, Dicom o cualquiera que lo requiera debe suscribir un contrato de licencia de uso de información con la Cámara de Comercio, en razón del cual se cobra un determinado precio por consulta. Todo el resto de los datos personales que maneja Dicom es obtenido de otras fuentes, las cuales pagan a Dicom por comunicar y mantener los datos personales de que se trate (esta base de datos es conocida como SICOM), salvo aquellos datos que pueden ser obtenidos de fuentes accesibles al público, como son por ejemplo, los registros del Conservador de Bienes Raíces de Santiago o el Diario Oficial, los cuales pueden ser recogidos sin cobro de tarifa alguna. Por último, otra fuente importante de información personal para esta empresa es el Estado; se han suscrito una serie de convenios de intercambio de información entre Dicom y algunos organismos estatales que si bien no tienen valor monetario o contable sí lo tienen desde un punto de vista económico, en estos convenios las partes se obligan a entregar recíprocamente ciertos datos personales que manejan, así es el caso por ejemplo del Servicio de Impuestos Internos, Servicios de Aduanas, Registro Electoral, Servicio de Registro Civil e Identificación. Así, por ejemplo, Dicom ofrece el servicio denominado "Registro de Infracciones y Anotaciones Tributarias"[357].

[356] EMOL EL MERCURIO. El negocio de las temidas bases de datos de incumplimientos comerciales. 2003 [en línea] <http://www.economiaynegocios.cl/tus_finanzas/tus_finanzas.asp?id=568&numero=14> [consulta: 14 febrero 2005].

[357] EQUIFAX. 2006. [en línea] <https://www.dicom.cl/dic/hom.01/pag/p.dic.hom.mas-productos-personas.htm#> [consulta: 14 febrero 2006].

Una vez que Dicom ha accedido y recogido los datos personales, los distribuye por medio de la venta a los usuarios finales que lo soliciten. De otra parte, los tipos de datos patrimoniales que entrega Dicom[358] son de la más variada índole: morosidades, protestos de documentos impagos, avalúo de bienes raíces, el hecho de ser socio de una sociedad, si se está impedido de abrir cuenta corriente, si se poseen bienes gravados con prenda sin desplazamiento, si se han cometido infracciones tributarias, si tienen juicios pendientes, entre otros.

Databusiness es un servicio de información personal de naturaleza patrimonial, que ofrece básicamente el mismo tipo de información que Dicom, agregando la morosidad de seguros. Sus fuentes de información son las mismas que Dicom. El público objetivo de databusiness es también compartido con Dicom.

Datarent es una base de datos de la Cámara de Comercio de Santiago que recopila, procesa y consolida la información de morosidades de los contratos de arriendo a nivel nacional. Esta base de datos es creada por los Corredores de Propiedades a través de un sistema computacional, utilizando la plataforma Internet. Los propios corredores ingresan y actualizan la información de morosidad, la cual queda registrada en la Base de Datos Datarent y puede ser consultada, posteriormente, a través de una empresa distribuidora de información comercial. Es interesante observar cómo en la página web de datarent se informa cuándo la recogida de datos personales que da cuenta de la morosidad derivada del incumplimiento por parte del arrendatario de la obligación del pago de la renta es legítima y cuándo no, se indica en la página *web*[359] en cuestión que "Aquellos corredores afiliados a asociaciones gremiales, tales como ACOP, podrán ingresar a la base de datos Datarent las morosidades superiores a 30 días, aunque no figure la cláusula correspondiente en el contrato. En este caso, por no existir cláusula, la información sólo podrá ser consultada a nivel interno por los asociados de la entidad." Lo anterior, se encuentra perfectamente acorde con lo establecido en el artículo 4 inciso final de la Ley 19.628 que faculta a las personas jurídicas privadas (asociaciones) a tratar datos 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. No pudiendo, conforme se colige del texto legal comunicar los

[358] Dicom no sólo vende o distribuye este tipo de datos, también lo hace con datos de identificación, laborales, y otros, que serán analizados más adelante.
[359] DATARENT. Preguntas Frecuentes acerca de datarent. http://www.datarent.cl/Inicio/Faq.htm> [consulta: 15 febrero 2005].

datos a terceros. Además indica la página web que "los particulares no podrán ingresar las morosidades de los arriendos en cuyos contratos no figure en forma previa la cláusula Datarent[360], ya que esto no cumple con lo dispuesto en la ley 19.628 que exige el consentimiento previo por parte del arrendatario." Cosa que es totalmente cierta, ya que si el particular no se encuentra en ninguna de las situaciones de excepción que contempla la ley citada, se debe aplicar el principio general para el tratamiento de datos que indica que se debe tener autorización previa del titular de los datos, para poder efectuar tratamiento de ellos. [361]

La asociación de bancos e instituciones financieras A.G. constituyó el 27 de octubre de 1987 la sociedad Sistema Nacional de Comunicaciones Financieras S.A. - SINACOFI, cuya finalidad principal es la administración, operación y desarrollo de una red electrónica, para apoyar en forma eficiente la acción comercial y operativa de las instituciones financieras de nuestro país, mediante el intercambio de información de valor[362]. Desde los inicios de la operación de la Red SINACOFI, se incorporaron todos los bancos y financieras que operan en el país, junto a los organismos reguladores y fiscalizadores del sector (Banco Central y Superintendencia de Bancos e Instituciones Financieras).

La información personal que maneja esta base de datos está compuesta especialmente por datos patrimoniales de naturaleza bancaria y financiera. Estos datos son recogidos de los propios bancos e instituciones que conforman la asociación, los cuales, a su vez, y en un principio eras los usuarios exclusivos de la información, ya que SINACOFI no distribuía los datos personales al público en general, sólo a sus asociados. Sin embargo, actualmente SINACOFI "es una sociedad cuyo objeto social contempla el desarrollo de actividades relacionadas con el procesamiento de datos mediante sistemas computacionales, sistemas automatizados de transferencia de información y la prestación de servicios de información a la industria bancaria y al mercado en general, bajo estándares de alta seguridad en su integridad,

[360] Llama la atención que la Cámara de Comercio de Santiago informa al público de la conveniencia de la utilización de la siguiente cláusula tipo en los contratos de arrendamiento: "Para el evento de incumplimiento del pago o simple retardo en el cumplimiento del pago de una cualquiera de las rentas convenidas en el presente contrato, queda facultada la arrendadora para publicar dicho incumplimiento o retardo en la base de datos del sistema Datarent. Esta autorización da satisfacción a lo establecido en el artículo 4° de la ley N° 19.628". DATARENT. Cláusula contractual datarent. 2005 [en línea] <http://www.datarent.cl/Inicio/Clausula.htm > [consulta: 15 febrero 2005].

[361] DATARENT. Preguntas Frecuentes acerca de datarent. 2005 [en línea] <.http://www.datarent.cl/Home.htm > [consulta: 15 febrero 2005].

exactitud y disponibilidad"[363]. Los datos que son puestos a disposición del público, son prácticamente los mismos que aquellos de sus competidores, a través de la denominada "Central de Riesgos", sólo habría que hacer especial mención a los datos relacionados con deudas y morosidades en el negocio del factoring[364].

La empresa Servicios Integrados de Información S.A. (SIISA), que nació a principios de la década de los 80' se ha convertido en el cuarto actor de relevancia en el mercado de datos personales. Su manera de operar respecto a la recogida de datos personales es similar a la de DICOM, como también lo es, los datos personales que conforman sus bancos de datos. La información personal la distribuyen a cualquier sujeto que lo solicite.

La Cámara de Comercio de Santiago es otro importantísimo actor en el mercado de datos patrimoniales, ya que maneja dos de las bases de datos de mayor tamaño y uso, la de las morosidades de las casas comerciales (INFOCOM) y la del Boletín Comercial, además de los sistemas de información databusiness y datarent.

Como se indicaba INFOCOM, es un servicio de información sobre las morosidades de los titulares de tarjetas de crédito de las siete mayores casas comerciales en Chile. La Cámara de Comercio de Santiago administra esta base de datos y distribuye a las empresas de bases de datos (Dicom, SIISA) los datos personales que contiene la señalada base de datos, las cuales entregan la información al usuario final, no obstante lo cual, el usuario final también puede comprar los datos personales directamente a la Cámara de Comercio de Santiago.

El Boletín de Informaciones Comerciales es administrado por la Cámara de Comercio de Santiago, y se encuentra regulado en el DS 950 del Ministerio de Hacienda de 1928. El señalado decreto autoriza a la Cámara a procesar y comunicar la siguiente información:

---

[362] ASOCIACIÓN DE BANCOS E INSTITUCIONES FINANCIERAS A.G. Sinacofi. 2005 [en línea] < http://www.abif.cl/menu-superior/filiales/sinacofi.htm> [consulta: 16 febrero 2005].

[363] SISTEMA NACIONAL DE COMUNICACIONES FINANCIERAS. 2006. [en línea] <http://www.sinacofi.cl/marco_legal.asp> [consulta: 14 febrero 2006].

[364] Los servicios completos se encuentran en SISTEMA NACIONAL DE COMUNICACIONES FINANCIERAS. 2006. [en línea] <http://www.sinacofi.cl/faq-central.asp> [consulta: 14 febrero 2006].

- Entregada por los Notarios: a) Estados que contengan la nómina de las letras protestadas durante el día, indicando si el protesto es por falta de aceptación o de pago, el monto de la letra, el nombre y domicilio del librado o aceptante y el nombre del girador. b) Lista de las compraventas, remates y adjudicaciones de bienes raíces, indicando los nombres de las partes contratantes, la ubicación de la propiedad y el precio de venta. c) Lista de los mutuos hipotecarios, con indicación de los nombres del deudor y del acreedor, la ubicación de la propiedad y monto del préstamo. d) Lista de las cancelaciones. e) Nómina de las nuevas sociedades comerciales organizadas y de las modificaciones y disoluciones de éstas. f) Convenios extrajudiciales entre comerciantes.

- Entregada por los Juzgados de Letras en lo Civil de mayor cuantía y los de menor cuantía: a) Nómina de los embargos, retenciones, quiebras y concursos que se decreten. b) Lista de las sentencias ejecutoriadas que condenen al pago de rentas insolutas de arrendamiento de bienes raíces. c) Nómina de los decretos de posesión efectiva que se otorguen.

- Entregada por los Conservadores de Bienes Raíces: Una nómina de las inscripciones practicadas durante el día, en los registros de propiedad; de hipotecas y gravámenes; de interdicciones y prohibiciones de enajenar de prenda agraria; y de prenda industrial. Junto con la nómina enviarán en extracto los detalles correspondientes fiscales, semifiscales o de administración autónoma, que realicen actividades destinadas a promover el desarrollo económico del país, enviarán una nómina de todos los deudores morosos en el servicio de préstamos o créditos. Asimismo, los bancos, sociedades financieras y administradoras de mutuos hipotecarios y cooperativas de ahorros y créditos podrán remitir la nómina de los deudores morosos en el servicio de sus préstamos o créditos. Estas nóminas se remitirán dentro de los quince primeros días de cada mes calendario y contendrán el nombre completo del deudor, Rol Unico Tributario, su domicilio y el monto del servicio que estuviere debiendo.

- Entregada por la Asociación Nacional de Ahorro y Préstamo: una nómina de los deudores que hayan incurrido en mora en el pago de sus dividendos hipotecarios, con indicación del número de dividendos no pagados, el monto total de ellos y el domicilio del deudor.

- Entregada por los bancos y sociedades financieras: a) Una nómina de las letras de cambio y pagarés, aceptadas o suscriptos con la firma autorizada por un Notario, a la orden del banco o de la sociedad financiera, no pagados a su vencimiento y que no hayan sido protestados por falta de pago por Notario u Oficial de Registro Civil, en su caso. b) Una nómina de las letras de cambio y pagarés que hubieren protestado estas instituciones a su vencimiento, en conformidad a lo dispuesto en la Ley número 18.092. Las nóminas aludidas precedentemente deberán contener los siguientes antecedentes: en el caso de las letras de cambio el monto de la letra, el nombre, Rol Único Tributario y domicilio del aceptante y el nombre del girador; en el caso de los pagarés, se deberá indicar su monto, el nombre y Rol Único Tributario del suscriptor.

Como se puede observar la gran cantidad y diversidad de información de naturaleza patrimonial, tanto negativa como positiva, respecto de la cual la Cámara de Comercio de Santiago está legalmente facultada para acopiar y tratar, hace de esta institución un actor vital en el mercado de datos personales, ya que se convierte en el único distribuidor de información que puede garantizar la posesión y calidad de los datos personales que maneja, debido básicamente a que los entes generadores de la información están obligados por el decreto supremo 950 a entregar la información en cuestión a la Cámara de Comercio de Santiago[365]. Debido a lo anterior, mucho se ha discutido en este último tiempo respecto de una suerte de monopolio legal por parte del Boletín Comercial. En el Congreso se discuten actualmente dos proyectos de ley que buscan derogar el referido decreto supremo, con el objeto de eliminar este monopolio legal, y tener de esta manera a un mercado de datos personales patrimoniales que presente libre competencia. Es así, como se indica en la moción de uno de estos proyectos que "Este Decreto Supremo crea importantes barreras, expresadas en la casi nula sustituibilidad en el mercado de las Informaciones Comerciales, tanto por el lado de la demanda (no existen productos suficientemente similares al Boletín Comercial en cuanto a su función, precio y atributos para

[365] A este respecto interesante resulta reproducir parte del contenido de la página web de la Cámara de Comercio de Santiago, en la cual señalan que la Ley 19.628 ratificó al Boletín Comercial en su papel de banco de datos único de protestos y morosidades, que cumple el rol de fuente oficial, lo cual es absolutamente falso, ya que como viéramos en el capítulo II sólo se indica que el la norma que regula esta Boletín aplicará en la medida en que no contradiga la Ley 19.628. Asimismo, indica la referida página web ciertas apreciaciones respecto del Boletín Comercial, señalando que éste cumple con la ley, al: a) Garantizar un justo balance entre la información necesaria para lograr la transparencia del mercado crediticio y la adecuada protección de la privacidad de las personas; b) Asegurar la veracidad y homogeneidad de la información y -por consiguiente- la confiabilidad del sistema; y c) Custodiar el cumplimiento de los plazos establecidos por la ley en relación a la vigencia de la información sobre los incumplimientos de las personas naturales. BOLETIN COMERCIAL. CAMARA

ser considerados por los usuarios como sustitutos), como así también por el lado de la oferta y la competencia potencial (ya que el carácter "oficial" que se le atribuye al Boletín Comercial impide la existencia de oferentes de información comercial perfectamente sustituibles a la Cámara de Comercio).” [366]

Por otra parte, en la discusión del proyecto de ley, el Presidente de la Cámara de Comercio de Santiago, don Carlos Jorqueira expresó que: “Respecto del mercado de la distribución de información, señaló que es un mercado en competencia con alto grado de concentración en un actor dominante, que es Dicom Equifax (80%), existiendo otras empresas distribuidoras, tales como Data Business, Sinacofi, y Siisa. Respecto de los indicadores de desempeño del boletín de informaciones comerciales, precisó que tiene un sistema computacional con los más altos estándares internacionales, que operan ininterrumpidamente por casi 80 años. La tasa de error de registros publicados, es del 0,004% y los errores de procesamiento interno, son solucionados vía Aclaración Especial, sin costo para el afectado. Respecto de los agentes crediticios, nunca hubo un requerimiento legal por errores o inconsistencia en la información publicada. En relación con los titulares de los datos, en promedio sólo hubo 3 acciones legales al año, en la última década y, en todos los casos, los Tribunales han dado la razón a la interpretación de la Cámara de Comercio de Santiago”.

Es por esta razón que el 18 de Mayo del 2005 la Fiscalía Nacional Económica presentó un requerimiento ante el Tribunal de Defensa de la Libre Competencia, en contra de la Cámara de Comercio de Santiago.

La presentación se funda en el abuso de la posición dominante de esta asociación gremial en el mercado de la información crediticia, materializado en el cobro de estas tarifas por las aclaraciones, las que para la Fiscalía son absolutamente ilegales y carecen de fundamentos económicos.

DE COMERCIO DE SANTIAGO. 2006. [en línea] <http://www.boletincomercial.cl/html/que_es_bic.htm> [consulta: 14 febrero 2006].

[366] Boletín 4159-03. Deroga el decreto supremo N° 950, del Ministerio de Hacienda, de 1928, sobre boletín comercial.

De nuestra parte, creemos que el mercado de datos personales patrimoniales ya no necesita que exista una ley que entregue a una determinada institución, en este caso, la Cámara de Comercio, el tratamiento, distribución y comunicación de este tipo de información, ya que existe actualmente la disposición a compartir información por parte de los acreedores, asimismo existe movilidad de los deudores y un buen grado de competencia.

Por último, debemos mencionar a la Superintendencia de Bancos e Instituciones Financieras (SBIF), como un representante de aquellos que distribuyen información personal patrimonial. La diferencia fundamental con los actores mencionados anteriormente, es que la SBIF, es un organismo público que, no obstante ello, opera en la práctica como una empresa privada ya que vende informes comerciales a quienes los soliciten, aun cuando a un precio menor que su competencia y se entrega el informe sólo a las personas afectadas, esto es, a los titulares de los datos personales. La información personal patrimonial que es distribuida por la SBIF, es más restringida que en los casos que analizáramos anteriormente, ya que sólo se refiere en el caso del informe de deudas, al endeudamiento de una persona con el sistema financiero y en el caso del estado de deudas (que encuentra fundamento legal en el artículo 14 de la Ley General de Bancos que obliga a la SBIF a mantener una información permanente y refundida sobre los deudores del sistema bancario para uso exclusivo de las instituciones financieras sometidas a su fiscalización[367]) a la individualización de los deudores y el estado de las deudas

[367] CHILE. 2002. Decreto con Fuerza de Ley N°3 que fija texto refundido, sistematizado y concordado de la Ley General de Bancos y de otros cuerpos legales que indica. Diciembre 1997. El señalado artículo 14 indica: "No obstante lo dispuesto en el artículo 7º y sin perjuicio de las normas sobre secreto bancario contenidas en el artículo 154, la Superintendencia deberá proporcionar informaciones sobre las entidades fiscalizadas al Ministro de Hacienda y al Banco Central de Chile. La Superintendencia dará también a conocer al público, a lo menos tres veces al año, información sobre las colocaciones, inversiones y demás activos de las instituciones fiscalizadas y su clasificación y evaluación conforme a su grado de recuperabilidad, debiendo la información comprender la de todas las entidades referidas. Podrá, también, mediante instrucciones de carácter general, imponer a dichas empresas la obligación de entregar al público informaciones permanentes u ocasionales sobre las mismas materias. Con el objeto exclusivo de permitir una evaluación habitual de las instituciones financieras por firmas especializadas que demuestren un interés legítimo, la Superintendencia deberá darles a conocer la nómina de los deudores de los bancos, los saldos de sus obligaciones y las garantías que hayan constituido. Lo anterior sólo procederá cuando la Superintendencia haya aprobado su inscripción en un registro especial que abrirá para los efectos contemplados en este inciso y en el inciso segundo del artículo 154. La Superintendencia mantendrá también una información permanente y refundida sobre esta materia para el uso de las instituciones financieras sometidas a su fiscalización. Las personas que obtengan esta información no podrán revelar su contenido a terceros y, si así lo hicieren, incurrirán en la pena de reclusión menor en sus grados mínimo a medio. En todo caso, los bancos y sociedades financieras deberán cumplir con la obligación que establece el artículo 9º de la ley Nº 18.045, sobre Mercado de Valores, sea que sus acciones estén o no inscritas en el Registro de Valores. En caso de incumplimiento de dicha obligación, podrá proporcionar la información la Superintendencia."
La Superintendencia deberá mantener permanentemente una nómina de los depositantes de los bancos, indicando su rol único tributario (RUT).

que mantienen en el sistema bancario en el mes al que se refiere. La deuda comprende el conjunto de obligaciones reales y contingentes de una persona natural o jurídica, sea por su calidad de deudor directo o indirecto, incluyéndose las deudas tanto vigentes como vencidas**.** Está constituida por el saldo de capital adeudado más los reajustes e intereses devengados hasta la fecha de referencia del Estado de Deudores[368]. La fuente de información primaria de la SBIF son todos los bancos e instituciones que están obligados a entregar la referida información a la Superintendencia, como asimismo, la asociación de bancos e instituciones financieras, a través de SINACOFI.

Como podemos observar de lo indicado respecto al mercado de datos personales patrimoniales, éste se caracteriza por tener pocos oferentes, teniendo sobre todo la Cámara de Comercio de Santiago un peso gravitante sobre los demás, debido a la gran cantidad de información que maneja y porque posee un monopolio legal sobre el Boletín de Informaciones Comerciales. De otra parte, ciertos órganos públicos como el Banco Central y la Superintendencia de Bancos e Instituciones Financieras, juegan un rol preponderante tanto como fuentes de información como distribuidores de ella.

Podemos señalar, para concluir, que en este mercado, dada la presencia de la Cámara de Comercio de Santiago, existe oligopolio ya que las decisiones que adopta la Cámara necesariamente van a influir el resto de los actores de este mercado, desde que ella es la principal fuente de información secundaria, como también, es uno de los más importantes distribuidores de información personal patrimonial, sin olvidar lo que ya comentáramos respecto de su monopolio legal sobre el Boletín de Informaciones Comerciales. En este mismo sentido se pronuncia Rony Jara al señalar que "Dado que la totalidad de las entidades que generan la información comercial comunicable, salvo el caso de las sociedades administradoras de crédito de las casas comerciales, se encuentran obligadas a enviar su información a la Cámara de Comercio de Santiago, para su publicación en el Boletín de Informaciones Comerciales, dicho banco de datos se convierte naturalmente en el principal generador de información comercial en el mercado. Cualquier otro competidor debe recurrir a dicha fuente matriz o acordar individualmente con cada productor de la información que obligatoriamente le es proporcionada

[368] SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS A.G. 2005 [en línea] <http://www.sbif.cl/sbifweb/servlet/AtencionPublico?indice=1.2.1.1&idContenido=996> [consulta: 16

por la Cámara. A su vez, y dada la obligación de aclaración que el artículo 19 impone al acreedor cuando se extingue la obligación adeudada por un modo en que intervenga directamente el acreedor, es lógico pensar que dicha aclaración se efectuará siempre, al menos, en el Boletín Comercial, puesto que como vimos será la fuente primaria de información comercial para todo el mercado."[369]

3.3. Mercado de datos con fines publicitarios o de marketing

Un importante porcentaje de los datos personales que son tratados en nuestro país, lo son con el objeto de efectuar publicidad o marketing directo, es decir, de promoción de bienes o servicios. Cada vez que una persona recibe en su hogar a través de correo tradicional un folleto, panfleto, cartola o cualquier aviso publicitario impreso, hay detrás un tratamiento de datos personales, la misma afirmación se aplica, cuando recibimos un correo comercial no solicitado o *spam*[370].

Aquellos que actúan en este mercado lo hacen a nombre propio, es decir, es la propia empresa que efectúa el marketing directo la que trata los datos personales, o bien, se trata de empresas especializadas en publicidad o marketing que tratan datos personales con el objeto de efectuar marketing directo como parte del servicio que ofrecen. Las fuentes de esa información son variadas; las empresas recaban datos de sus clientes o potenciales clientes, a través de contratos, formularios, fuentes de acceso público, etc., siendo relevante en este punto el acceso a bancos de datos personales o más bien la compra de bases de datos ilegales, esto es, que no cumplen con la Ley 19.628 o que han sido obtenidas por medios ilícitos, las que se efectúan en una suerte de mercado negro[371]. Rodolfo Herrera, a propósito de las fuentes de información en el

---

febrero 2005].

[369] JARA, Rony. op.cit. pág. 78.

[370] El *spam* y el marketing directo efectuado por Internet será analizado cuando nos refiramos al mercado de datos personales en la Red.

[371] El hito más importante respecto a la compraventa de bancos de datos personales en el mercado negro, ocurrió en el año 1995, en el mes de abril, cuando Falabella sufrió el hurto de su base de datos de clientes, la cual contenía, más de un millón de registros con la situación laboral, los ingresos, la capacidad los ingresos, la capacidad de endeudamiento, los bienes y la puntualidad de pago de sus clientes. Una vez que Falabella presentó las respectivas querellas, se constató la sustracción de un cartridge de respaldo desde sus oficinas. Este fue traducido y reducido a disquettes, con el fin de ser vendidos a empresas de la competencia. La compañía Top Marketing fue la encargada de comercializar los registros con distintas casas comerciales. De todas las nombradas en el proceso, la única transacción comprobada por la justicia -y cuya suma ascendía a los $ 3,5 millones- fue hecha por La Polar, empresa que se encuentra actualmente procesada. El caso sentó un importante

marketing directo indica que se explota una enorme cantidad de datos desordenados obtenidos de fuentes tan diversas como las de acceso público, del tráfico y la facturación, de la relación comercial establecida por las partes u otras, señalando que se utilizan tres técnicas en el sector del marketing directo y que dicen relación con el tratamiento de datos personales: datawarehouse, el datamining y el DSS [372].

Los tipos de datos personales que se manejan en el marketing directo, son aquellos que permiten identificar y ubicar a una determinada persona, ya sea en el espacio real o virtual (nombre, domicilio, rut, teléfono, correo electrónico), como aquellos que permiten efectuar perfiles de las preferencias o gustos de un sujeto (compras que efectúa con la tarjeta de crédito, páginas web que suele visitar, respuestas directas en encuestas o formularios, entre otras)[373].

---

precedente para legislar en detalle, años más tarde. REVISTA QUE PASA. Chilenos al desnudo. 2000. [en línea] <http://64.233.161.104/search?q=cache:0Tl29o0NZJ:www.quepasa.cl/revista/1511/36.html+%22datos+personales%22+%22marketing+directo%22&hl=es > [consulta: 16 febrero 2005].
Otro ejemplo de utilización indebida de bases de datos con el objeto de realizar marketing directo es el caso Nic Chile- Acepta.com. Respecto de este caso, el sitio web de Nic Chile publica la siguiente declaración conjunta con Acepta.com: "En Santiago de Chile, a 15 de Mayo de 2001, los señores Patricio Poblete, Director de NIC Chile y don Roberto Opazo Gazmuri, en su carácter de gerente general de Acepta.com, han considerado oportuno efectuar la siguiente declaración pública:
En abril del año 2001 la empresa Acepta.com inició una campaña de marketing directo utilizando el correo electrónico como canal de comunicación, la cual fue considerada por un sector de la comunidad como "spam". En el contexto de esta campaña se enviaron e-mails a las casillas que Acepta.com logró recolectar de diferentes sitios Web, incluyendo en ella, parte de la información publicada por NIC Chile.
Las direcciones de correo electrónico disponibles en el sitio Web de NIC Chile son publicadas con el único fin de apoyar la administración y funcionamiento de nombres de dominio y por lo tanto su uso para una campaña de marketing directo es improcedente y constituye un error que Acepta.com reconoce haber cometido actuando de buena fe, por el cual ofrece disculpas a NIC Chile y a sus usuarios.
Las direcciones de correo electrónico de los usuarios de NIC Chile han sido eliminadas de la Base de Datos de Acepta.com y esta fuente de información no será ocupada en el futuro para campañas de marketing. Adicionalmente, Acepta.com mejorará su política de marketing directo para incorporar una serie de sugerencias recibidas durante este proceso.
Considerando lo anterior, NIC Chile acepta las disculpas ofrecidas y ambas organizaciones concuerdan en que la situación producida ha quedado completamente superada." DECLARACIÓN CONJUNTA NIC CHILE- ACEPTA.COM. 2001. [en línea] http://www.nic.cl/anuncios/2001-05-15.html [consulta: 15 febrero 2006].

[372] HERRERA, Rodolfo. 2001. Digitalización y convergencia: el nuevo entorno de las telecomunicaciones. [en línea] <http://www.adi.cl/pdf/digyconv.pdf> [consulta: 16 febrero 2005]. Indica el *datawarhouse* posibilita aglutinar una serie de diseños de bases de datos que agrupan un gran volumen de información optimizada para su explotación. Así, el almacenamiento de datos organizado permite combinar todas las fuentes de información relevantes para una organización en una única estructura de base de datos susceptible de apoyar el proceso estratégico de la información. El *datamining* o minería de datos es el análisis efectivo de los datos almacenados, que descubre relaciones sutiles u ocultas entre elementos que constituyen la información de las bases de datos, así como la generación de modelos predictivos derivados de ellos. Los DSS o *Decisión Support Solutions,* son aplicaciones para el análisis de un gran volumen de datos y la realización de gran variedad de cálculos y proyecciones.

[373] La empresa Mapcity ofrece en su sitio web apoyo a la gestión comercial de las empresas mediante el uso de herramientas de análisis geoestadístico, basado en información de mercado y su asociación a planos digitales. Así, por ejemplo, el servicio de *Database Marketing* ofrece: "Procesos de

Respecto a la importancia de las bases de datos personales de clientes a efectos publicitarios en nuestro país, se ha declarado que "Las bases de datos de clientes, cuya utilización antecede al comercio electrónico, se han transformado en herramientas fundamentales del actual modelo de negocios, dando origen a la personalización extrema del marketing, denominada *marketing-to-one*…la llamada "minería de datos" (metáfora de la extracción de metales preciosos del subsuelo) se ha transformado en toda una industria, como lo ejemplifica la compañía canadiense Air Miles, que se especializa en obtener información sobre hábitos de compra ofreciendo en el punto de venta bonos que los clientes acumulan y pueden canjear por pasajes de avión, minutos de larga distancia, etc."[374]

En algunos países en donde se ha reconocido la importancia que han adquirido las bases de datos personales para las actividades publicitarias y el marketing, se ha reconocido a la vez, la necesidad de respetar la privacidad de los titulares de los señalados datos. Por ejemplo, en España[375] y México[376] los mismos que se dedican a este tipo de actividades empresariales o comerciales, han dictado normas autorregulatorias en lo que respecta a la utilización de datos personales con fines de marketing directo. En nuestro país, si bien algunas asociaciones y/o corporaciones como la CONAR (Consejo de autorregulación y ética publicitaria) poseen código de ética, en él no se hace referencia al tratamiento de datos personales con fines de publicidad directa[377].

---

enriquecimiento, de confiabilización, de normatización y de duplicación de Base de Datos, Diseño de Modelos de Datos, Análisis y Segmentación Poseemos bases de datos de personas con información actualizada respecto de direcciones y teléfonos, para contactabilidad, segmentadas por grupo socioeconómico, grupo etáreo, zona geográfica, etc." MAPCITY. 2004-2005. [en línea] <http://www1.mapcity.com/empresa_geo.php> [consulta: 16 febrero 2005].

[374] CÁMARA DE COMERCIO DE SANTIAGO Economía Digital. 2000 [en línea] <http://www.ccs.cl/html/actualizar/Estudios/edigtal.PDF > [consulta: 16 febrero 2005].

[375] La Asociación Española de Comercio Electrónico, en su código de ética, regula en el Título IV la protección de datos personales en este ámbito. ASOCIACIÓN ESPAÑOLA DE COMERCIO ELECTRÓNICO. CÓDIGO DE ÉTICA. 2005 [en línea] < www.aece.org/docs/codigo.pdf> [consulta: 18 febrero 2005].

[376] La Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, tiene un código de ética cuyo artículo 23 sobre adopción y puesta en práctica de una política de privacidad indica que: "Todos los socios de la AMIPCI cuya actividad se encuentre orientada hacia el comercio electrónico o a establecer actividades en línea, tienen la responsabilidad de adoptar y poner en práctica un conjunto de políticas para proteger la privacidad de los Datos Personales (en adelante: DP). Deben también tomar medidas para fomentar la adopción y puesta en práctica de políticas de privacidad para cualquier otra organización relacionada, que incluye compartir esa filosofía con socios comerciales y clientes." ASOCIACIÓN MEXICANA DE LA INDUSTRIA PUBLICITARIA Y COMERCIAL EN INTERNET. CÓDIGO DE ÉTICA. 2005 [en línea] < http://www.amipci.org.mx/amipci/codigo_de_etica.html > [consulta: 18 febrero 2005].

[377] CONSEJO DE AUTORREGULACIÓN Y ÉTICA PUBLICITARIA. CÓDIGO DE ÉTICA. 2005 [en línea] <

3.4. Mercado de datos de identificación

Existe un mercado cada vez mayor de datos de identificación. Consideramos que son tales aquellos datos que sirven para poder singularizar o identificar a una persona, haciéndola determinada, como por ejemplo, el Rol Unico Tributario o la Cédula Nacional de Identidad, el nombre, la dirección o domicilio, teléfono, datos biométricos como las huellas digitales o el iris. Dicom/Equifax en el ámbito privado se dedica en forma más visible y organizada a la venta de este tipo de información (excluyendo datos biométricos), ofreciendo cruzar datos como el teléfono, cédula de identidad y nombre de una persona para obtener una "relación entre ellos". Las fuentes de esta información personal que son declaradas por Dicom son: el fisco, empresas aportantes de información y los propios titulares de datos cuando efectúan algún tipo de trámite como un bloqueo por ejemplo[378]. Sin embargo, el mayor actor de este mercado es el Estado; múltiples órganos públicos como el Registro Electoral, el Servicio de Impuestos Internos, y actualmente el Servicio de Registro Civil e identificación, venden los datos de identificación que poseen de los ciudadanos a través de la firma de contratos de prestación de servicios, a empresas que luego, utilizan esa información personal para usos propios, o bien, sirven de canales de distribución de los datos personales que compran. Todo lo anterior, a través de procesos automatizados de comunicación.

3.5. Mercado de datos personales en Internet

Otro de los mercados dentro de los cuales la utilización de datos personales ha ido en constante crecimiento es el de Internet. En la Red, la información personal de los navegantes o usuarios es tratada ya sea a partir de una recolección directa de los datos, teniendo como fuente al propio titular de ellos que entrega su información en forma voluntaria y consciente, o bien, a través de lo que la doctrina denomina tratamiento invisible de datos personales, que consiste en un conjunto de operaciones y procedimientos técnicos efectuados por programas y equipos

---

http://www.conar.cl/p4_portada/antialone.html?page=http://www.conar.cl/p4_portada/site/artic/20031124/pags/20031124163705.html > [consulta: 18 febrero 2005].

[378] DICOM. Dicomguías. 2005 [en línea] <https://www.dicom.cl/dhom/pag/p.hom.000.f-productos.htm> [consulta: 29 marzo 2005].

capaces de procesar los datos de los usuarios y ponerlos a disposición de terceros sin conocimiento o consentimiento de sus titulares[379].

Cuando una persona navega por Internet, sus datos personales como hábitos de consumo y preferencias, van siendo recogidos en forma invisible a través de una serie de herramientas informáticas, tales como Applets de Java, Javascript integrado en el código fuente HTML de la página web, Cookies y Controles ActiveX, Visual Basic, etc.

Entre los datos obtenibles con Applets de Java y Javascript, figuran la dirección de correo electrónico, tipo de navegador, versión del mismo e idioma, sistema operativo, resolución de pantalla, fuentes, nombre asignado al computador, dirección IP fija o dinámica, número de páginas visitadas y URL de procedencia.

Entre los datos obtenibles con ActiveX y Visual Basic, figuran el historial de navegación; datos de identificación del usuario, introducidos durante la instalación y configuración del programa navegador, o del programa correo electrónico, o cualquier otro; direcciones de correo electrónico de otros usuarios; y, bases de datos y agendas electrónicas[380].

Como señalábamos, además de esta recolección invisible de datos, existe aquella que se efectúa con conocimiento y consentimiento del titular, cuando éste entrega voluntariamente sus datos personales a través de formularios, encuestas y otros. Aun cuando, en esencia, a ambos tipos de recolección de datos se les aplica la misma legislación, debemos de reconocer, que la recogida invisible de datos a través de Internet u otra plataforma electrónica, es potencialmente más lesiva a la privacidad del titular de los datos que se recolectan, ya que éste desconoce que sus datos están siendo tratados, y quién lo está haciendo.

A continuación mencionamos, las actuales y más comunes formas de adquisición invisible de datos personales en Internet:

---

[379] HERRERA, Rodolfo. 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].
[380] RIBAS, Javier. Riesgos Legales en Internet, especial referencia a la protección de los datos personales. EN: Derecho de Internet. Madrid, Ed. Aranzadi. 2001 pág. 154.

Las *cookies* son un conjunto de caracteres que se almacenan en el disco duro o en la memoria temporal del computador de un usuario cuando accede a las páginas de determinados sitios *web*. Se utilizan para que el servidor al que se ha accedido pueda conocer las preferencias del usuario al volver éste a conectarse. Los navegadores que existen actualmente en el mercado permiten, en todo caso, desactivarlas[381], sin embargo, son pocos los usuarios que se encuentran familiarizados con la utilización de estas herramientas técnicas pro-privacidad.

Las *cookies* buscan determinar cuáles son los hábitos de navegación de un determinado usuario, de manera, de poder registrar cuáles son sus gustos, a qué hora suele navegar en Internet, qué tipos de sitios visita y cuáles no, etc.

Los denominados *spyware* (software de espionaje o software espías) son programas computacionales, que se instalan en computadores, sin el conocimiento o consentimiento del usuario, generalmente cuando se bajan de Internet ciertos software gratuitos o *freeware*.

La función esencial de estos programas es detectar los hábitos de navegación del usuario del PC en donde se instalan, de manera, que cada cierto tiempo, que ha sido previamente programado, envían a través de Internet al servidor que también ha sido predeterminado (utilizando las redes que son pagadas por el mismo usuario) la información recolectada sobre el usuario, para ello, a los usuarios se les asigna un GUID (Globally Unique IDentifier o Identificador Global Único), de manera de poder distinguir la actividad que cada usuario en particular ejecuta en la Red.

Es así como estas empresas que proveen software gratuito, pagan sus costos a través de la utilización y comercialización de los datos personales o información que obtienen a través de los *spyware*.

---

[381] DICCIONARIO DE TÉRMINOS INFORMÁTICOS [en línea] http://www.moheweb.galeon.com/diccinformatic.htm#C [consulta: 29 marzo 2005].

Cada día los *spyware* se están haciendo más comunes. Hay estudios de expertos informáticos[382] que indican que cerca del 90% de los computadores con conexión a Internet en el mundo estarían "infectados" con este tipo de programas espías.

El *adware* es una especie de *spyware*, pero que tiene fines de publicidad. A través del *adware*- nuevamente- se pueden obtener las costumbres de navegación de una determinada persona, sólo que acá el objeto de la recolección es mandar publicidad dirigida o costumizada al usuario, a través de ventanas de publicidad o *pop-ups*, que van siguiendo al navegante aun cuando se cambia a otra página web.

Para determinar si este tipo de técnicas que implican un tratamiento invisible de datos caen bajo el amparo de la Ley 19.628, es necesario recordar lo dicho en el capítulo II respecto a propósito de los datos estadísticos o disociados, esto es, aquellos que no pueden asociarse a persona identificada o identificable, a los que no se les aplica la protección que brinda la Ley, al no considerársele datos personales. En consecuencia, cabe preguntarse si estos programas involucran sólo un tratamiento de datos disociados o si permiten asociar los datos que recogen a una persona determinada o determinable, por ejemplo, a través de un número de IP fijo. Si no lo permiten, el tratamiento de datos en cuestión no queda regulado por nuestra legislación protectora de datos. Si lo permiten, será discutible si una dirección IP implica identificación de una persona o la hace identificable, ya que estas direcciones van cambiando y son asignadas por el proveedor de acceso a Internet.

En razón de lo anterior, en muchas de las políticas de privacidad de sitios o páginas *web*, se utilizan frases como las que siguen: "nuestras cookies se asocian únicamente con un Usuario anónimo y su ordenador, y no proporcionan por sí el nombre y apellidos del Usuario" o "el sitio web reúne información de navegación de los usuarios, la cual es automáticamente recolectada por el mero hecho de estar en nuestro site y que es información que carece de datos personales y no se puede asociar a la identidad de una persona física".

En consecuencia, si bien es cierto que en la gran mayoría de los casos no estamos en presencia de infracción a la Ley 19.628 cuando se utilizan estos programas, la privacidad e

[382] EARTHLINK. 2005. [en línea] http://www.earthlink.net/spyaudit/press/ [consulta: 29 marzo 2005].

intimidad de las personas, en tanto "el derecho a poder estar solo si uno lo desea, a mantenerse apartado de la observación de los demás sin ser molestado, sin intromisiones en lo más personal de su vida"[383], sí parece ser, a lo menos, amenazada.

Otra de las técnicas que se utilizan en el mercado de Internet, sobre todo, a efectos de publicidad o marketing y que implica efectuar un tratamiento de datos personales, es el envío de correos electrónico no solicitados, también conocido como correo basura, *spam* o *junk mail*. Los altos costos que se generan debido al espacio que ocupan en las redes, servidores y computadores de los usuarios y al tiempo que se utiliza en borrarlos, es indiscutido. A este respecto cabe citar el estudio efectuado ya en el año 2002 por la Cámara de Comercio de Santiago, según el cual, Chile perdía anualmente la suma de 36,1 millones de dólares por las prácticas de *spam*[384].

Legislaciones de otros países, como la norteamericana, han optado por penalizar esta conducta. En nuestro país, el *spam*, se encuentra regulado indirectamente en la Ley 19.628 y de manera directa en la Ley 19.496, sobre protección a los derechos de los consumidores, a través de una modificación reciente efectuada a la ley[385].

Para que los *spamers* puedan efectuar el envío de correos electrónicos en forma masiva, necesariamente deben tratar datos personales. El dato personal utilizado es la dirección de correo electrónico del afectado por el *spam*. El correo electrónico es un dato personal, según el concepto que de él efectúa la Ley 19.628, porque constituye información que se refiere a una persona identificada o identificable (el titular de la cuenta de correo). Con la dictación de la Ley 19.628, se "legalizó" en buena medida el envío de *spam*, ya que el artículo 4 señala que no requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

---

[383] VERDUGO, M; PFEFFER, E.; NOGUEIRA, H. op.cit. pág.250.

[384] EL MERCURIO DE VALPARAÍSO. 2002. [en línea] <http://www.mercuriovalpo.cl/site/edic/20021129205118/pags/20021130010226.html> [consulta: 12 marzo 2008].

[385] La Ley 19.496 fue modificada por la Ley 19.955 publicada en el Diario Oficial el 14 de julio de 2004.

Para analizar la legalidad del *spam*, a la luz de la Ley 19.628, debe distinguirse la fuente de la cual el *spamer* extrajo la dirección de correo electrónico: Así, si se extrajo de cualquier fuente que no sea de acceso restringido o reservado, no necesitará autorización de su titular. En cambio, si se extrajo de una fuente reservada o no pública, sin autorización del titular, el tratamiento de datos y envío de *spam* es ilegítimo.

Hay que tener presente que la sola entrega voluntaria de la dirección de correo electrónico no implica la legitimación para efectuar tratamiento de datos respecto de ella, si no ha mediado previamente autorización expresa del titular de los datos a efectos de efectuar tratamiento, y en los términos exigidos por el propio artículo 4 de la ley citada.

Como señalamos, el *spam* también se encuentra regulado en la ley sobre protección a los derechos de los consumidores, cuyo artículo 28 B, indica: "Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos."

Se instituye como opción legislativa la técnica del *opt-out*, esto es, que los *spamers* pueden enviar libremente correos electrónicos a los consumidores-usuarios, mientras éstos no soliciten la suspensión de tales envíos; luego de lo cual, el envío de correos electrónicos por ese mismo *spamer* a ese mismo consumidor-usuario constituirá infracción a la ley, que se encuentra sancionada con multa de hasta 50 unidades tributarias mensuales.

Además, se obliga a que en estas comunicaciones promocionales - entendiendo por tales las prácticas comerciales consistentes en el ofrecimiento al público en general de bienes y servicios en condiciones más favorables que las habituales, con excepción de aquellas que consistan en una simple rebaja del precio - o publicitarias - las comunicaciones que el proveedor dirige al público para informarlo y motivarlo a adquirir o contratar un bien o servicio – que se señale: la materia o asunto sobre el que versa; la identidad del *spamer* o remitente; y, una dirección electrónica válida. La falta de alguno de estos requerimientos en el correo electrónico publicitario o promocional, constituye una infracción a la ley.

Respecto al ámbito de aplicación de esta normativa, surge la duda si ella es de general aplicación a todo *spam*, ya que utiliza la frase "Toda comunicación promocional o publicitaria enviada por correo electrónico", o bien, dado el ámbito de aplicación de la ley, debe entenderse que sólo se aplica a aquellos correos electrónicos que, siendo comunicaciones promocionales o publicitarias: i) sean enviados a consumidores (personas naturales o jurídicas que, en virtud de cualquier acto jurídico oneroso, adquieran, utilicen o disfruten, como destinatarios finales, bienes o servicios); ii) tengan carácter de onerosos (ofrezcan bienes o servicios no gratuitos), y iii) impliquen la existencia de un acto jurídico mercantil para el *spamer* y civil para el consumidor-usuario.

La segunda interpretación implica que parte importante de los correos electrónicos no deseados quedan fuera del ámbito de aplicación de la ley, tales como aquellos que se envíen a personas naturales o jurídicas que no sean los destinatarios finales de los bienes o servicios que se ofrecen; los que tengan una naturaleza gratuita, como un mail en que se invita a un charla gratuita; los de campañas políticas, etc. Creemos, que esta interpretación es la correcta.

Por último cabe indicar, que se ha presentado por el Senador Jovino Novoa un proyecto de ley[386], cuyo contenido en muy discutible, y que tiene por objeto modificar la Ley 19.628 en varios aspectos, uno de ellos dice relación con el *spam*. Respecto a él, indica el proyecto que "eleva a la categoría de dato sensible la dirección de correo electrónico". Creemos que en esta parte el proyecto de ley en comento yerra, ya que la dirección de correo electrónico se encuentra muy alejada de la naturaleza que tiene aquella información que sí es sensible, y que se caracteriza fundamentalmente porque su tratamiento implica un peligro al permitir y aumentar la posibilidad que se produzca discriminación arbitraria entre las personas. Lo señalado anteriormente es corroborado por el derecho comparado, ya que no existe ninguna norma que catalogue al correo electrónico como información sensible.

[386] Boletín Nº 3796-07. Proyecto de ley iniciado por el Honorable Senador señor Novoa, que 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 resguardar a los usuarios de correos electrónicos de la propaganda comercial no solicitada.

3.6. Mercado de datos médicos

Denominamos datos médicos a aquella información de naturaleza personal y sensible, que se encuentra contenida en las recetas médicas prescritas a los pacientes y a aquella referida a la compras de medicamentos que efectúan las personas en farmacias o establecimientos afines.

En nuestro país, una empresa de estudios de mercados de salud internacional con presencia en Chile, IMS[387], se dedica a comercializar esta información a las empresas farmacéuticas. Son diversas las formas a través de las cuales recaban la información: a través de promotoras en las mismas farmacias que solicitan la autorización del paciente a efectos de copiar su receta médica; a través de convenios con farmacias que le entregan la información respecto de las recetas que llegan a su poder y a través de convenios con empresas de seguros de salud, que también le proveen esta información[388]. En los dos últimos casos existen autorizaciones generales por parte de los pacientes en las cuales permiten la copia y revelación de los datos contenidos en las recetas.

Luego esta información es vendida a aquellos que presenten interés en conocer qué están recetando los médicos y qué medicamentos están comprando los pacientes; obviamente el principal cliente de esta empresa son las farmacéuticas, quienes utilizan la información para conocer qué están recetando los médicos y optimizar sus ventas.

3.7. Mercado de datos personales públicos

Todos los órganos del Estados manejan información de naturaleza personal de los ciudadanos y como ya esbozáramos varios de ellos efectúan transacciones en el mercado en base a la referida información personal que manejan. A continuación analizaremos algunos de los casos más emblemáticos.

---

[387] IMS lleva tiempo en el mercado. Fue creada en 1954 en los Estados Unidos y su valor de mercado en 2005 bordeó los US$ 5.000 millones. Además, figura 898 en el ranking de la revista Fortune de las 1.000 compañías más grandes de Norteamérica. ELMERCURIO.COM 2006. [en línea] <http://www.economiaynegocios.cl/noticias/noticias.asp?id=85255> [consulta: 25 marzo 2006].

a) Servicio de Impuestos Internos (SII)

El SII declaró ante el Servicio de Registro Civil e Identificación, poseer las siguientes bases de datos: i) de bienes raíces el cual contiene los datos legales del propietario (nombre y rut) y datos físicos catastrales que permiten determinar el avalúo del bien raíz; ii) ciclo de vida del contribuyente, que contiene un registro de inicio de actividades y participación en sociedades, legalización de documentos y términos de giro efectuados por los contribuyentes ante el Servicio de Impuestos Internos; iii) registro de pagos, declaraciones y devoluciones de impuestos que contiene datos tributarios, registros de los impuestos (IVA, Renta, otros) declarados y pagados por los contribuyentes; y, iv) registro de contribuyentes que contiene Incluye todas las personas jurídicas y naturales, chilenas y extranjeras, según nombre, rut, fecha de nacimiento o de constitución de sociedad, nombres y apellidos, razón social[389].

Como ya señaláramos, Dicom y otras empresas del rubro informan sobre datos de las personas, en su calidad de contribuyentes. Así por ejemplo, se informa respecto de las infracciones y anotaciones tributarias, a cualquiera que lo solicite previo el pago correspondiente. Lo anterior, se debe a que el SII ha suscrito con diversas empresas privadas como, por ejemplo, Dicom, convenios de intercambio de información. La suscripción de los referidos convenios se encuentra amparada por la legalidad establecida respecto de ellos por la Contraloría General de la República, quien indicó como respuesta a un requerimiento efectuado por dos diputados que "atendido que el Servicio de Impuestos Internos cuenta con atribuciones para celebrar contratos, que la información que se proporciona en virtud de los convenios aludidos no tienen el carácter de secreta o reservada, sino que es información pública (número de rol único tributario de los contribuyentes, nómina de los contribuyentes con incumplimiento tributario, avalúos de los bienes raíces, tasación de vehículos y timbraje de documentos), que en tales contratos se adoptan los resguardos necesarios para que esa información no sea utilizada para objetos no queridos por el Servicio, y que esa repartición pública, fundadamente, ha estimado necesario la celebración de estos acuerdos para el mejor cumplimiento de sus

[388] ELMERCURIO.COM 2006. [en línea] <http://diario.elmercurio.com/2006/03/20/editorial/tribuna/noticias/39103DB6-DE1A-4A4E-A144-2C429C717E71.htm> [consulta: 25 marzo 2006].
[389] SERVICIO REGISTRO CIVIL E IDENTIFICACION. CONSULTA. 2005. [en línea] <http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html> [consulta: 15 febrero 2006].

funciones, cabe concluir que en la materia analizada el Servicio de Impuestos Internos actúa dentro de sus facultades legales."[390]

Asimismo, resultan interesantes ciertos argumentos de naturaleza económica esgrimidos por la Contraloría para fundamentar su dictamen, así se indica que: "es posible constatar, de los informes del Servicio de Impuestos Internos, como de los demás antecedentes que se han tenido a la vista, que la necesidad de dar a conocer estos datos se explica por el deber que tiene esa entidad de evitar la evasión tributaria. En efecto, se señala que la evasión proviene de actos realizados por personas que se encuentran en situación tributaria irregular, lo que redunda en el uso de documentación tributaria falsa o no fidedigna, el no ingreso en arcas fiscales de los impuestos correspondientes y el incumplimiento de normas tributarias. La publicidad, por tanto, permite que las decisiones contractuales o de otro orden se tomen con antecedentes que permitan realizarlas con una razonada evaluación del riesgo de estar incurriendo en incumplimiento de las normas tributarias, disminuyendo así la evasión y aumentando la recaudación. Se añade que resulta conveniente para los fines del Servicio aprovechar las empresas especializadas que existen en el país, dedicadas a prestar servicios de información desde sus bancos de datos, para que a través de ellas los contribuyentes puedan informarse respecto de la situación tributaria de las personas naturales y jurídicas con que se relacionan, evitándose así el Servicio los costos pertinentes y aumentando la cobertura de control tributario. También se señala que para el mejor cumplimiento de la función fiscalizadora resulta útil, también, tener acceso a los bancos privados de información, ya que el incumplimiento de las obligaciones por los agentes económicos constituye un indicador objetivo que demuestra un patrón de conducta que, proyectado a la satisfacción de las obligaciones tributarias, permite a ese Servicio orientar y planificar programas preventivos de control respecto de determinados contribuyentes o grupos de éstos."[391]

Como se puede observar, varios de los argumentos de la Contraloría miran a obtener un mayor grado de eficiencia en el actuar fiscalizador del SII, como asimismo, a tomar decisiones contractuales de menor riesgo al conocer a aquellos que incumplen con sus obligaciones de naturaleza tributaria.

[390] Dictamen número 10.322 de fecha 21.03.2001 de la Contraloría General de la República.
[391] Ibídem.

b) Tesorería General de la República (TGR)

Al igual que el SII la TGR celebra con empresas privadas convenios de intercambio de información, cuya legalidad también ha sido establecida por la Contraloría con símiles argumentos a los revisados respecto del SII, así la Contraloría dictaminó que la TGR "se encuentra habilitada para suscribir con empresas especializadas que manejan bases de datos, acuerdos de voluntades para intercambiar información relativa a contribuyentes y deudores que se encuentran en mora con el Fisco, dado que la referida información no tiene el carácter de secreta ni reservada, sino que es pública"[392] requiriendo eso sí que "en tales acuerdos se adopten los resguardos necesarios para que tal información no sea utilizada en finalidades distintas a las deseadas por el servicio y no se vulneren, además, las disposiciones que regulan la información de carácter secreto o reservada."[393]

En la práctica el sistema opera entregando la TGR a Dicom la información de deudores morosos a quienes se ha notificado mandamiento de ejecución y embargo, previendo de esta manera eventuales quejas por vulneración de la privacidad, ya que el asunto se hace público como cualquier expediente en tribunal. Dicom no paga por la información entregada por la TGR, pero sí facilita información económica y financiera pertinente sobre deudores[394].

c) Servicio Electoral

Una de las bases de datos públicas que ha sido puesta a disposición de más empresas privadas dedicadas a la venta de información es la del registro electoral[395]. Este organismo público afirma realizar venta de bases de datos a privados, lo cual esgrimen tiene fundamento legal en la Ley 18.768, que establece normas complementarias de administración financiera, de

[392] Dictamen número 43.866 de fecha 03.10.2003 de la Contraloría General de la República.
[393] Ibídem.
[394] "Intimidad y nuevas tecnologías. Análisis de la tutela efectiva a los derechos de los titulares de datos personales en Chile". Concurso de Ciencias Sociales, Humanidades y Educación DID 2002. pág. 249.
[395] Así por ejemplo lo informa Dicom en su sitio web. DICOM HOME. 2006. [en línea] <https://www.dicom.cl/com/com.01/pag/p.com.com.cons-dir-pers-p.htm>> [consulta: 15 febrero 2006].

incidencia presupuestaria y de personal, del Ministerio de Hacienda, la cual en su artículo 83[396] los faculta para percibir ingresos propios.[397]

Entendemos que de las bases de datos que maneja este Servicio, sólo pueden comunicar a terceros aquella denominada "padrón alfabético computacional", que contiene datos (nacionalidad, fecha de naciomiento, RUN, nombre y apellidos, sexo, discapacidad visual, ocupación, profesión) de los chilenos mayores de dieciocho años inscritos en los Registros Electorales y extranjeros, mayores de dieciocho años, avecindados en Chile por más de cinco años e inscritos en los Registros Electorales, ya que el resto de los bancos de datos que manejan, son reservados o secretos, como por ejemplo, el Registro General de Afiliados a partidos políticos o el Registro de los inscritos condenados o procesados a pena aflictiva[398].

d) Servicio de Registro Civil e Identificación (SRCI)

El SRCI es el organismo público más activo en el mercado de datos personales, ya que no sólo funciona por medio de la suscripción de convenios de intercambio de información como los revisados respecto del SII o TGR, sino que además, vende directamente acceso a información personal de sus bases de datos a cualquier empresa que lo solicite y que cumpla con los requisitos técnicos y contractuales que el contrato de adhesión que creó el SRCI establece a estos efectos.

---

[396] Artículo 83.- Sustitúyese el artículo único del decreto ley N° 2.136, de 1978, modificado por el artículo 63 de la ley N° 18.681, por el siguiente:
"Artículo Unico.- Facúltase a los servicios dependientes de la Administración Central y Descentralizada del Estado, del Poder Legislativo y del Poder Judicial, para cobrar el valor de costo de los documentos o copias de éstos que proporcionen a los particulares para la celebración de contratos, llamados a licitación o por otra causa, y cuya dación gratuita no esté dispuesta por ley, sin perjuicio de mantener a disposición de los interesados los respectivos antecedentes cuando ello proceda. También podrán cobrar por la producción de fonogramas, videogramas e información soportada en medios magnéticos, sus copias o traspasos de contenido.
Los recursos provenientes de estos cobros constituirán ingresos propios de las instituciones mencionadas."

[397] "Intimidad y nuevas tecnologías. Análisis de la tutela efectiva a los derechos de los titulares de datos personales en Chile". Concurso de Ciencias Sociales, Humanidades y Educación DID 2002. pág. 248.

[398] Todas las bases de datos que maneja este servicio han sido comunicadas al Servicio de Registro Civil e Identificación y pueden ser visitadas en la página web de este último servicio. SERVICIO REGISTRO CIVIL E IDENTIFICACION. 2006. [en línea] <https://www.registrocivil.cl/OficinaInternet/servlet/MuestraPagina?contexto=1&pagina=/Institucion/convenio_con_empresas/ConveniosEmpresasInstituciones.html> [consulta: 16 febrero 2006].

De acuerdo a lo informado en la propia página web del SRCI "Existen una serie de servicios disponibles que permiten validar la información que poseen las entidades externas con la contenida en los registros de este Servicio. La información disponible contempla las consideraciones habidas en la Ley N °19.628 de la Ley de Protección de Datos de la Vida Privada. De acuerdo lo dispone el artículo 7 letra i) de la Ley N °19.477, que aprueba la Ley Orgánica del Servicio del Servicio, es necesario suscribir un "Contrato de Prestación de Servicios" entre el Servicio de Registro Civil e Identificación (SRCeI) y la entidad que requiera la información, en el cual se establecen las responsabilidades de ambas partes, la forma de entrega de la información y su valor."[399]

Los servicios ofrecidos son los siguientes:

- Estado de vigencia de documentos de identidad
- Búsqueda de placa patente única por rut.
- Conectividad con municipios
- Consulta de anotaciones vigentes de vehículos
- Consulta de datos de registro civil: nacimientos, defunciones, matrimonios.
- Información estadística del registro de vehículos motorizados.

Además de estos servicios, el SRCI está trabajando en un nuevo servicio de verificación de identidad o biométrico, en base asimismo, en la suscripción de estos contratos de prestación de servicios. A partir de este servicio, que utiliza como datos de entrada los contenidos en la cédula de identidad y la huella digital, el SRCI pretende informar sobre:

- Fotografía
- Firma
- Impresión dactilar (solo para policías, y otros casos que la ley determine y también a quien el SRCI determinase)
- Datos alfanuméricos de la cédula de identidad (nombre completo, fecha de nacimiento, sexo, nacionalidad, fecha de emisión del

[399] SERVICIO REGISTRO CIVIL E IDENTIFICACION. 2006. [en línea] <https://www.registrocivil.cl/OficinaInternet/servlet/MuestraPagina?contexto=1&pagina=/Institucion/

documento, fecha de vencimiento del documento, número de serie del documento, número de inscripción del nacimiento, circunscripción del nacimiento y profesión)

- Decadactilar (10 impresiones dactilares rodadas, solo para las policías y en otros casos que la ley determine y también a quien el SRCI determinase)

Por otro lado, se ofrece el servicio de verificación de identidad en base a huella digital que funciona así: Por cada R.U.N. consultado más impresión dactilar en formato WSQ o minucia NEC, más identificación del dedo, el SRCI procederá a verificar la identidad realizando una comparación de AFIS 1:1. En este caso la respuesta será de los tipos: "Aprobado" o "No se puede efectuar verificación automática de identidad".

Como se puede observar son múltiples lo servicios que ofrece este organismo público de acceso a información personal de los ciudadanos previo pago de los cargos correspondientes. Respecto a estos servicios surgen dudas de legalidad en dos sedes, las cuales sólo serán planteadas ya que ahondar en ellas excede el objeto de este capítulo: i) Infracción al artículo 20 de la Ley 19.628, ya que este comercio de los datos personales de los ciudadanos no se encuentra dentro de la competencia del SRCI, y por lo tanto, requiere de autorización previa del titular; y ii) Infracción al artículo 19 Nº 21 inciso segundo de la Constitución Política de la República, ya que claramente este organismo del estado está realizando una actividad económica, para la cual no ha sido autorizado mediante la ley de quórum calificado que exige la norma de la carta fundamental.

Finalmente y respecto de los organismos públicos en general cabe consignar la jurisprudencia administrativa de la Contraloría General de la República, que sienta el principio general en materia de tratamiento y cesión de datos personales por organismos públicos, al señalar en varios de los dictámenes revisados que: "la sola circunstancia de que un servicio público efectúe tratamiento de datos personales -materia que regula la Ley N° 19.628 y entendida como cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que, en general, le permitan el manejo más eficiente de la

convenio_con_empresas/ConveniosEmpresasInstituciones.html> [consulta: 16 febrero 2006].

información que tiene a su cargo-, no implica que el respectivo servicio público se encuentre facultado para ceder esos datos a terceros, posibilidad ésta que debe ser examinada con sujeción a la naturaleza de la información de que se trate y a la competencia del órgano pertinente"[400].

3.8. Conclusiones

Es claro que en nuestro país existe un mercado de datos personales de la más diversa índole tanto por el tipo de dato con el cual se comercia, como asimismo, por la variedad de actores que intervienen en la referida comercialización. A primera vista este mercado está funcionando de una manera eficiente, sin embargo creemos que algunos aspectos del modelo regulatorio deben de ser cambiados para lograr realmente la eficiencia[401].

[400] Dictámenes de la Contraloría General de la República Nº 42.760 de 16.11.2001; Nº 10.322 de 21.03.2001 y Nº 43.866 de 03.10.2003.
[401] Este tema será revisado en profundidad en los próximos capítulos.

CAPITULO IV

ANÁLISIS ECONÓMICO DEL MERCADO DE DATOS PERSONALES Y SU REGULACIÓN

4.1. Fundamentos económicos para un mercado de datos personales

Como lo señalan Kay-Lung-Hui y I.P.L. Png[402], desde una perspectiva económica, los gobiernos, empresas y otras organizaciones usan la información personal, principalmente, con tres objetivos:

a) Para "customizar" bienes y servicios, discriminando más efectivamente entre personas con diferentes intenciones de pago o diferentes ingresos, como asimismo, clasificar más efectivamente entre personas con diferentes características.

b) Para usar la información personal en un mercado para uso propio del que la recolecta o de otros en otro mercado (vendiéndola).

c) Para marketing.

En relación con estos usos, encontramos en la literatura sobre la materia diversos argumentos que establecen el porqué debe existir un mercado de datos personales, o dicho en otros términos, porqué es eficiente o deseable contar con información personal de terceros en distintos ámbitos, aun cuando debemos señalar que la mayoría de los referidos argumentos se refieren a datos de naturaleza patrimonial o a tratamiento de datos con el objeto de efectuar marketing.

En primer lugar, se indica que es eficiente y atractivo el tratamiento de datos personales, porque estamos hablando acá de información, la cual como vimos en el capítulo I de la presente tesis, reviste ciertas características de bien público que resultan deseables para las empresas

demandantes de la referida información (excluyendo a aquellas que "crean" la información por primera vez), así se ha señalado que: "Una vez producida la información puede ser usada muchas veces a bajo costo por diferentes actores, esta característica de bien público, es una fuente importante de la productividad de la información. Los usos múltiples a bajo costo que permite la información, hace que diversos demandantes de ella, como por ejemplo, instituciones de crédito, empresas aseguradoras y publicistas usen la misma información personal; es más, ellos cooperan en generar esta información, porque todos ellos la consideran valiosa. Desde que los usos múltiples de la información se subsidian unos a otros, más información es recolectada y el costo para cada uno de los usuarios de ella es menor"[403].

Luego, se señala que el poseer información personal es eficiente en el mercado de créditos en relación a la determinación del riesgo, tanto para el titular del banco de datos como para el titular de los datos personales, ya que "La información proveída por los distribuidores de datos personales patrimoniales es usada para otorgar crédito eficientemente entre los potenciales solicitantes de él. Los distribuidores cumplen esta función de variadas formas. En primer lugar, proveyendo información acerca del historial de crédito del solicitante, creándoles una reputación en el mercado. Los solicitantes que no han cumplido sus obligaciones saben que su información de crédito estará disponible para instituciones de crédito en el futuro y sus posibilidades de solicitar crédito serán reducidas. Lo anterior, les incentiva a pagar sus créditos, lo que otorga a las instituciones de crédito mayor seguridad de que sus créditos serán pagados. En segundo lugar, los distribuidores evitan la selección adversa, ya que si la información de crédito no estuviera disponible algunos solicitantes obtendrían créditos sin intención de pagarlos. Las instituciones de crédito no tendrían la información para identificar a este tipo de solicitante y como resultado, el préstamo no ocurrirá, y si ocurre, las instituciones de crédito se verán forzadas a cargar grandes cantidades debido al riesgo que asumen. Por último, incluso los solicitantes con buenas intenciones pueden verse obligados al incumplimiento. Pero la probabilidad que esto ocurra varía entre los solicitantes. Las instituciones de crédito ganan situando a los solicitantes en la clase de riesgo apropiada y cobrando tasas de interés conformes al riesgo. Esto significa que el riesgo bajo paga bajas tasas y viceversa. Lo anterior, implica más

[402] Hui, Kai-Lung y Png, Ivan. op.cit. pág. 5.
[403][403] RUBIN, Paul. y LENARD, Thomas. Privacy and the commercial use of personal information. Washington DC, The Progress & Freedom Foundation. 2001.92p. pág. 9.

créditos y produce ganancias a los solicitantes de ellos. Estos mismos argumentos aplican al mercado de seguros[404][405].

Hal Varian quien ha escrito variados trabajos sobre la materia, indica como uno de los beneficios de poseer información personal la disminución de los costos de búsqueda, sobre todo, relacionados con el mercado de datos con fines publicitarios o de marketing[406]. Sin embargo, los autores[407] no sólo vislumbran beneficios para aquellos que efectúan tratamiento de datos personales, sino que también para sus titulares: "los titulares de datos y los que efectúan publicidad directa dirigida o *marketing to- one* se ven beneficiados por el tratamiento de datos personales, ya que los primeros reciben información que se ajusta a sus intereses, así como también no reciben información que no les interesa, y los segundos, porque ellos no están interesados en realizar publicidad dirigida a aquellos que no están interesados en ella. De otra parte, este tratamiento de datos, permite que el titular de ellos, reciba servicios valiosos sin cargo, como por ejemplo, información en línea, software gratuitos, catálogos de productos, etc." [408]

---

[404] RUBIN, Paul y LENARD, Thomas. op.cit. pág. 9.

[405] Estos mismos argumentos fueron esgrimidos por las Asociaciones de Aseguradores, Dicom y otras empresas, en la discusión del proyecto de ley chileno que regula esta materia, en orden a lograr que se pudiera efectuar libremente –esto es, sin autorización previa- tratamiento de estos tipos de datos personales. Lo anterior es expuesto por Rony Jara al señalar: "Durante la tramitación del proyecto de ley, numerosas entidades –asociaciones de aseguradores, de prestadores de salud, etc.- plantearon al legislador la relación entre información y riesgo, argumentando que mientras mayor era la información con la que se contaba, la determinación del riesgo asumido resultaba mucho más precisa, en consecuencia las tarifas que se cobraban podían tener una mayor correlación con los riesgos que se asumían en cada caso en particular. Ello implicaba, se señaló, un beneficio para aquellos usuarios que de lo contrario debían asumir un costo mayor por un riesgo al que no contribuían. El argumento es correcto, en efecto, una mayor determinación del riesgo necesariamente debería implicar una mayor eficiencia en la fijación de la respectiva tarifa. Desde una perspectiva jurídica también podríamos decir: "mayor información…mayor justicia en la determinación de los precios". JARA, Rony. op.cit. pág. 63.

[406] VARIAN, Hal. 1996. Economic aspects of personal privacy. [en línea] <http://www.sims.berkeley.edu/~hal/Papers/privacy/> [consulta: 02 febrero 2005].

[407] En el ámbito nacional también se ha reconocido estos beneficios, aun cuando restringido al ámbito de Internet. Iñigo de la Maza ha indicado que "La posibilidad de discriminar el mercado beneficia, en principio, a consumidores y a quienes ofrecen sus productos y servicios a través de la red. En el caso de la publicidad a medida por ejemplo, los consumidores tienen la posibilidad de recibir información sobre artículos respecto de los cuales manifiestan alguna preferencia, de esta manera se reducen los costos de transacción adscritos a la búsqueda de esos productos y se evita el envío y exhibición repetitiva de publicidad que no presenta interés para el usuario. En el caso de los productores esta información les permite averiguar las preferencias de sus consumidores a bajo precio, posibilitando la adecuación de sus productos a las necesidades de éstos. La sumatoria de estos beneficios permitiría a la economía, según prominentes economistas, funcionar con menor fricción a través de la disminución de los precios y un mayor dinamismo en la adecuación de los productos a las necesidades de los usuarios". DE LA MAZA, Iñigo. op.cit. pág. 270.

[408] RUBIN, Paul y LENARD, Thomas. op. cit. pág. 8.

En nuestro ámbito, Renato Jijena ha señalado la existencia de un interés legítimo de 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 quiénes tienen SIDA al momento de fijar políticas de salud, y los particulares, generalmente constituidos por empresas de servicios o entidades gremiales, que para asegurar la vigencia de un orden público económico necesitarán conocer los intereses comerciales irregulares o negativos de las personas que actúan en la vida comercial"[409].

Asimismo, durante la tramitación del proyecto de ley se indicó por Jaime Guerrero (abogado y fiscal de Dicom de la época) que existían dos grandes beneficios producidos por el tratamiento de datos personales patrimoniales: la democratización del crédito y la mantención de tasas de interés en niveles aceptables. Lo primero debido a que "una información ágil, oportuna, expedita, cierta y veraz… contribuyó a que una mayor cantidad de personas accedieran al crédito bancario, financiero y comercial"[410], lo segundo, es afirmado debido a que la información aminora el riesgo, y por lo tanto, permite cobrar tasas de intereses menores que no internalicen un riesgo mayor ante una menor cantidad de información.

De otra parte, algunos autores señalan que las utilidades económicas de la información personal han disminuido rápidamente; menos personas leen los correos no solicitados o los *banners* publicitarios, la tasa es menor al 0,5%, y por otro lado, los consumidores son actualmente más reticentes a dar sus datos personales que en el pasado[411]. Podría señalarse que existe más información personal que la eficiente en el mercado.

Ya respecto del importante punto referido a la cantidad eficiente de información personal en el mercado[412], Loretta Nott[413] indica a propósito de la información financiera[414] que

[409] JIJENA, Renato. op.cit. pág. 87. Respecto al reconocimiento que la Ley 19.628 efectúa de la conveniencia social de los registros o bancos de datos ver. VIAL, Felipe. op.cit. pág. 25.
[410] GUERRERO, Jaime. La empresa privada y la magistratura ante la acción de hábeas data. Revista Ius et Praxis. Universidad de Talca. Año 3. N° 1: 209-218. 1997. pág. 211.
[411] SHOLTZ, Paul. Transaction costs and the social costs of online privacy. [en línea] 2001. First Monday. Vol. 6. number 5. http://firstmonday.org/issues/issue6_5/sholtz/index.html [consulta: 10 febrero 2005]. pág. 11.
[412] Como indican Paul Rubin y Thomas Lenard "Implícita en las propuestas de regular el mercado de la información personal está presente la existencia de una "falla de mercado" que resulta en que "mucha" información está siendo producida, divulgada y usada". RUBIN, Paul y LENARD, Thomas. op. cit. pág. 9. Sin embargo, estos autores son partidarios de señalar que a mayor cantidad de información mayor eficiencia, cuando indican "Desde un punto de vista general, sin embargo, los

aunque su intercambio puede generar beneficios económicos, la valuación de esos beneficios por parte de los titulares de datos puede diferir dependiendo de las preferencias individuales acerca de la privacidad. Algunos titulares de datos pueden no sentirse cómodos compartiendo su información personal con compañías financieras, mientras otros pueden estar dispuestos a entregar sus datos personales a cambio de mejores servicios y productos. Desde el punto de vista de la empresa, la magnitud del valor económico generado por compartir información personal puede diferir entre las distintas empresas. Así, para algunas empresas ofrecer un gran grado de privacidad a sus clientes puede ser muy costoso hasta el nivel de perder ganancias económicas.

Indica esta autora, aplicando la teoría económica que existirá una cantidad eficiente de información en el punto donde los beneficios económicos de la información son balanceados contra los costos asociados a ella. Específicamente, si el valor económico creado por la información excede el valor derivado de la privacidad financiera, la teoría económica señala que esta situación es eficiente. En contraste, si el valor económico generado por las instituciones financieras en razón del acceso y uso de la información financiera de los titulares de datos no excede el beneficio que esos titulares obtienen de su privacidad financiera, entonces la eficiencia económica dictamina que esa información no debe ser compartida.

Asimismo, se ha indicado que los costos de transacción y la asimetría de la información llevan a una sobre revelación de información privada por parte de los titulares de datos y consecuentemente a una excesiva adquisición de ellos. Consideremos los estímulos frente a una empresa que adquiere información personal. Esa empresa gana el beneficio neto de utilizar la información, por ejemplo, en sus propios esfuerzos de marketing o en el pago que recibe cuando vende la información a terceros. Como la empresa interioriza las ganancias (en términos de su propio marketing o por el precio que recibe de terceros cuando vende la información) de utilizar

---

mercados funcionan mejor con más información. Cuando los costos de la información bajan, los actores del mercado obtienen más de ella, y, consecuentemente, toman mejores decisiones". Ibídem.

[413] NOTT, Loretta. Financial privacy: an economic perspective. Report for Congress order code RL31758. 2003. [en línea] <HTTP://www.epic.org/privacy/glba/RL31758.pdf> [consulta: 02 febrero 2005].

[414] Entendemos que a efectos de lo expuesto por esta autora, podemos aplicar sus mismos razonamientos a cualquier otro tipo de información personal.

la información, pero a su vez externaliza las pérdidas (la pérdida de la privacidad de los individuos), tendrá un incentivo sistemático para usar demasiada información personal[415].

Otros autores[416] establecen la eficiencia en la información personal existente en el mercado, no sólo desde un punto de vista cuantitativo, sino que también funcional, así indican: "En general, la venta de información respecto de los consumidores es más beneficiosa cuando el potencial de esa información es alto, por ejemplo, cuando la clasificación de los consumidores puede ayudar a ajustar las ofertas de los vendedores y los intereses de los consumidores. Si la información no causa un mayor intercambio eficiente en el mercado secundario, entonces vale la pena no efectuar su venta, lo que a su turno desalentará la recolección de información en el mercado primario".

En nuestro ámbito, Rony Jara se ha pronunciado, asimismo, respecto del nivel óptimo de información, pero efectuando el análisis desde la perspectiva de bien público que tendría la información, así establece que "Entonces el problema con estos bienes, por una parte es que si se otorga un monopolio sobre ellos puede darse una infraproducción, porque hay pocos incentivos para invertir en algo que los demás pueden usar libremente. Por el contrario, si se otorga el monopolio, y por lo tanto se cobra un precio, el problema puede ser que exista un consumo inferior al óptimo. De este modo, buscando un equilibrio, se debería llegar a una fórmula donde se proteja la información, si ello es condición para que se produzca, pero no hay que protegerla si en cualquier caso se produciría"[417].

Desde nuestro punto de vista, y conforme a los principios económicos generales podemos afirmar que efectivamente existe una sobreproducción de informacional personal, debido a diversos factores: el más importante de ellos es el que señala que los que efectúan tratamiento de datos no internalizan los costos que genera para el titular de los datos el uso que hacen de su información personal, por lo cual existe una brecha entre el costo marginal privado y el costo marginal social, generado por la externalidad negativa producida por aquellos que

[415] SWIRE, Peter. Markets, self regulation, and government enforcment in the protection of personal information. [en línea] Privacy and Self-Regulation in the information age. U.S. Department of Commerce, June 1997. <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm> [consulta: 18 febrero 2006]. pág. 4.
[416] Hui, Kai-Lung y Png, Ivan. op. cit. pág. 24.
[417] JARA, Rony. op. cit. pág. 62.

efectúan tratamiento de datos, lo que no entrega un óptimo social a la economía. Además, frente a la existencia de costos de transacción significativos pasa a ser relevante cómo se han asignado los derechos de propiedad por la ley, y dado que tales derechos no se encuentran bien asignados (a los que más valúan los datos personales) se produce entonces un nivel no óptimo de producción para la sociedad.

De esta manera, podemos señalar que existen ciertas características propias del mercado de datos personales, que explican en parte su existencia:

- El mercado de datos personales aparece como uno en el cual el bien que se transa -la información personal- puede ser compartido por los diversos actores a un bajo precio, ya que una vez producida las posteriores transacciones son de bajo costo debido a que la información personal posee ciertas características de bien público.

- La información personal es necesaria para el mercado, en especial, para el mercado de créditos y seguros, ya que minimiza el riesgo de las operaciones y con ello las primas asociadas a los créditos de consumo e inversión, como asimismo la de los seguros, disminuyendo las tasas de interés de estos mercados, lo que resulta beneficioso tanto para los que efectúan el tratamiento de datos personales como para los titulares de la información personal.

- El mercado de datos personales disminuye los costos de transacción, en particular, los costos de búsqueda respecto de potenciales contratantes, consumidores, clientes, proveedores, etc.

Finalmente, a nuestro entender se debe tener presente que existe en el mercado de datos personales una sobreproducción de información personal, esto es, no se produce el nivel eficiente de ella, situación que se genera debido fundamentalmente a la existencia de externalidades negativas para los titulares de datos que no son internalizadas por los que

efectúan el tratamiento de la información personal, de manera que en este mercado el costo marginal privado es menor al costo marginal social.

Ya revisados los fundamentos para la existencia de un mercado de datos personales, a continuación nos referiremos a cuáles son sus fallas y la necesidad o no de regular este mercado.

4.2. Fallas del mercado de datos personales

Diversos autores se han pronunciado sobre las fallas del mercado de datos personales, ya sea estableciendo la existencia de ellas o bien rechazando que tales fallas existan.

Peter Swire[418], entrega una doble visión de las fallas del mercado, de una parte indica que el fracaso del mercado se ha definido con respecto a los derechos humanos y de otra respecto de enfoques contractuales a la protección de información personal. Bajo los derechos humanos, la meta es proteger el derecho de los individuos a la privacidad según la teoría moral que define el derecho. El mercado fallará cuando proteja la privacidad menos de lo que es deseable bajo la teoría moral. Bajo el enfoque contractual, que es el que seguimos en esta tesis, la meta es que todos los individuos tengan igual nivel de información y por lo tanto tengan igual poder de negociación. En este sentido, para este autor el mercado generalmente falla debido a las asimetrías de información entre el que efectúa tratamiento de datos y el titular de ellos, así señala ”los costos de información se presentan debido a la asimetría de información existente entre la empresa y el consumidor, la empresa generalmente sabe mucho más que el consumidor sobre cómo la información será usada por la empresa” y de otra parte, reconoce la existencia de altos costos de transacción al señalar que “el consumidor puede enfrentar costos significativos por el simple hecho de tratar de entender la naturaleza de las políticas de privacidad de una empresa”.

Para Loretta Nott[419] en el mercado de la información financiera, las dos más relevantes fallas del mercado son las externalidades y la información imperfecta[420]. Indica que algunos economistas han postulado que no hay externalidades en el mercado de la información financiera

[418] SWIRE, Peter. op. cit. pág. 4.
[419] NOTT, Loretta. op.cit. pág. 6.
[420] Creemos que estas fallas de mercado se aplican a cualquier información personal que se encuentre en el mercado, y no sólo a la de naturaleza financiera.

desde que el intercambio de información que ocurre entre consumidores y las instituciones financieras no afecta a terceras partes. Sin embargo, para esta autora este punto de vista no considera el beneficio que las instituciones financieras reciben de acceder a la información que es intercambiada entre consumidores e instituciones no-financieras. La información financiera es un subproducto de transacciones que no son efectuadas con dinero tradicional, y, cuando éstas son incluidas en bases de datos, generan valor para las instituciones financieras cuando la comparten con sus afiliadas u otras empresas. Así, efectuando una analogía, indica que el beneficio económico obtenido por las instituciones financieras, es similar al beneficio que obtiene una persona cuando su vecino pinta su casa. En tanto las instituciones financieras no compran esta información, están recibiendo una externalidad positiva por poder acceder y usar la información financiera[421]. De su parte, esta autora indica que existe asimetría de información en el mercado de la información financiera debido a que es posible que los titulares de datos no conozcan completamente el valor de mercado de su información financiera con la misma extensión que las instituciones financieras[422].

En relación al valor de la información personal y las fallas de mercado, Paul Schwartz[423] indica que la discriminación de precios en el mercado de la privacidad implica la existencia de empresas que efectúan tratamiento de datos y que distinguen entre los individuos en base a sus preferencias acerca del uso de sus datos personales, sin embargo, una falla presente en este mercado es la imposibilidad de observar tales preferencias por las empresas, dejando en consecuencia, a los consumidores con la sola posibilidad de elegir entre permitir o prohibir el tratamiento de sus datos personales.

Para ilustrar este punto, este autor toma dos consumidores: A, a quien le importa realmente cómo se usa su información personal, y B, que no. Un excedente de cooperación bajo un régimen de propietarización requiere como mínimo, que A y otros con similares preferencias reciban más que su valor de amenaza para así revelar sus datos personales. El término valor de

[421] Otro ejemplo de externalidad positiva es dado por RUBIN, Paul y LENARD, Thomas op. cit. pág. 11, al indicar: "Desde que la información permite múltiples usos una vez producida, muchas actividades que utilizan información producen externalidades positivas. Hay externalidades positivas asociadas al *marketing to-one*. La posibilidad que cualquier publicista tiene de obtener la información necesaria para mejorar el *marketing to-one* que efectúa, produce beneficio a otros publicistas, lo que es una externalidad positiva."
[422] NOTT, Loretta. op. cit. pág. 7.

amenaza se refiere al precio por no revelar su información personal. Actualmente, sin embargo, las empresas generalmente no necesitan ofrecer más bienes, servicios o dinero por sus datos personales a A que a B. Este fenómeno, de hecho, se presenta en los modelos de telemarketing. A y B tendrían sólo dos opciones, ellos se pondrían rehusar al telemarketing o escuchar sus llamadas sin compensación. Así, las firmas de telemarketing no necesitan distinguir entre los consumidores con diferentes preferencias acerca de su privacidad, pero deben alcanzar a todos los individuos de igual manera.

De este modo, podemos concluir que en el mercado de datos personales no existe discriminación de precios, ya que las empresas no pueden distinguir las preferencias de los individuos acerca del uso de sus datos personales.

Desde otro punto de vista y con bastante fundamento, se señala que la asimetría de la información se produce en desmedro de los que efectúan tratamiento de datos "El mercado de créditos y el mercado de seguros son potencialmente objetos de asimetría de la información, porque vendedores y aseguradores tienen menos información que los solicitantes de crédito o seguros acerca de sus características que puedan implicar riesgo en la operación de crédito o seguro. En general, el uso creciente de datos personales resuelve, antes que exacerba, los problemas de asimetría de la información"[424].

Para Paul Schwartz[425] la asimetría de información en el mercado de datos personales se produce porque las empresas coleccionan los datos de los individuos sin el conocimiento de éstos. La ignorancia de los individuos produce que una de las partes pertenecientes al mercado de la información de datos ni siquiera se entere que existió una "negociación" que se llevó a cabo. Incluso, si existe una sensación de que los datos han sido coleccionados, muchos individuos no saben cómo o de qué manera estos datos fueron procesados y compartidos.

Este mismo autor[426] señala que los que efectúan tratamiento de datos poseen incentivos para utilizar estrategias que hagan que sea difícil para los titulares de datos poder obtener una

[423] SCHWARTZ, Paul. Property, privacy, and personal data. 2004.Harvard Law Review. 117: 2056-2128. pág. 2077.
[424] RUBIN, Paul y LENARD,Thomas. op. cit. pág. 10
[425] SCHWARTZ, Paul. op.cit. pág. 2078.

información comprensible acerca de la recolección de datos y su uso. El problema con la asimetría de información es que ésta puede sistemáticamente trabar negociaciones y producir lo que los economistas denominan "equilibrio limón": una vez que la asimetría de información cause un número suficientemente grande de compradores que cesen de comprar, los vendedores perderán dinero como resultado de su decisión de ofrecer mejores términos de contrato a un precio más alto. El resultado es un equilibrio limón que ocurre cuando el mercado ofrece sólo malos productos (o "limones") para vender o presenta sólo malos términos de contrato, principalmente debido a que ningún vendedor tiene incentivos a ofrecer el contrato más favorable[427].

Comparte Iñigo de la Maza[428] el criterio que señala que el mercado falla como respuesta definitiva al problema de la privacidad, fundamentalmente por dos razones expuestas por Paul Schwartz: la existencia de vacíos de conocimiento y falacia del consentimiento. La primera razón, se presenta porque rara vez los sujetos poseen conocimiento sobre el hecho que su información será utilizada o la forma en que será utilizada (esto es, asimetría de información)[429], la segunda razón señala que para que el consentimiento tenga alguna relevancia para atar la libertad de los individuos precisa ser informado y voluntario.

Siguiendo con el postulado sobre la asimetría de información que afecta a los titulares de datos, E. Rose[430] señala que los que efectúan tratamiento de datos poseen más información acerca de lo que se reúne y cómo la información es utilizada y compartida en relación a los titulares de datos. Debido a los altos costos de monitoreo que poseen los titulares de datos éstos necesitarían incurrir en gastos muy altos para reducir esta asimetría en el mercado secundario. Como resultado, los titulares de datos deben soportar los costos sociales tales como comprar y

---

[426] SCHWARTZ, Paul. op. cit. pág. 2080.
[427] El efecto limón se puede explicar con el siguiente ejemplo: imaginemos dos bienes de distinta calidad: alta y baja. Los compradores creen que la mitad de los bienes son de baja calidad, y por lo tanto, los valoran a un menor precio, mientras que la otra mitad de los bienes la valoran en un mayor precio por ser bienes de alta calidad. Para un comprador típico el valor del bien seleccionado es un promedio entre el precio más alto (mejor calidad) y más bajo (menor calidad). Por lo anterior, el comprador no está dispuesto a pagar el verdadero valor de un bien de alta calidad, debido a que el bien puede ser "limón" o de baja calidad. El dueño de un limón estará deseoso de vender por el margen de ganancia entre el precio verdadero de su bien, imaginemos $100 y el precio promedio $150, no así, el dueño de un bien de alta calidad, que se valúa en $200, y que no está dispuesto a vender a $150. Una falla de mercado asociada a esta asimetría de información entrega como resultado la sola existencia de vendedores de bienes de baja calidad.
[428] DE LA MAZA, Iñigo. 2002. op.cit. pág. 274.
[429] El paréntesis es nuestro.

aprender a utilizar las tecnologías para aumentar la privacidad, evitar el robo de la identidad, llamadas de publicidad sin interés, etc. La solución para los titulares de datos que experimentan la violación de su privacidad es reducir la asimetría de información. Los niveles actuales de información asimétrica y externalidad positiva que favorecen a los que efectúan tratamiento de datos siguen existiendo en el mercado secundario. Por lo tanto, las leyes de la protección de datos que darían a los titulares un mayor control, podrían permitir la aplicación de derechos individuales de propiedad y tratar así a la información personal como un bien cuasi-privado, es decir un bien que es no-rival y excluible.

Hal Varian, ofrece otro punto de vista respecto a este tema, para él los usos múltiples o secundarios de la información producen externalidades negativas y ejemplifica, señalando que las acciones de una parte que compra una lista de correos electrónicos, potencialmente impondrá costos a los individuos que se encuentran en esa lista, pero el comprador de la lista en cuestión ignoró esos costos cuando la vendió. Estos costos, continúa este autor, podrían ser mitigados en alguna medida si el individuo que está en la lista de correos tiene derecho a voz en la transacción y ejemplifica señalando que el individuo puede prohibir cualquier uso secundario de su información personal, o por ejemplo, puede permitir distribuir su información a aquellas empresas o personas que le interese.

Kenneth Laudon[431] señala que la falla del mercado de datos personales es la asimetría en el poder y en la información, la cual se configuraría porque existe un lucrativo mercado de información personal, en el cual generalmente los individuos no participan debido a que no tienen intereses de "propietarios" en él, como asimismo, no poseen herramientas para influir en las instituciones que utilizan su información. Laudon afirma que los costos de transacción en que incurren las grandes empresas para obtener datos personales son menores y en disminución, mientras que los costos de transacción en que incurren los titulares de datos, incluso para conseguir una copia del dato son muy altos. Este autor afirma abiertamente que las legislaciones sobre privacidad en los últimos veinte años han reafirmado las fallas del mercado al asegurar los

[430] ROSE. Ellen. op.cit pág. 2.
[431] 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. 1.

intereses propietarios en la información personal al que efectúa el tratamiento de datos y denegándoselos al titular de ellos.

Para este mismo autor en este mercado existen externalidades negativas para los titulares de datos, las cuales son experimentadas por ellos como un costo directo e indirecto excesivo producido por la reproducción de información. Da algunos ejemplos de costos tangibles como el de excesivo correo, pérdida de atención, y como costos intangibles, la pérdida de serenidad, privacidad y soledad. Señala, por último, a este respecto que estas externalidades negativas deben ser compensadas con las externalidades positivas que produce una casi ilimitada explotación de información personal como las enormes cantidades de información publicitaria que es despachada a los consumidores (tanto si éstos lo desean o no). Sin embargo, arguye, que no puede señalarse que estas externalidades positivas compensan completamente a los titulares de datos o a la sociedad por los costos negativos de una explotación sin límites de la información personal[432].

Finalmente haremos referencia a la interesante postura del profesor Michael Froomkin, quien denomina a la "*privacy myopia*" como una de las causas de la existencia de fallas de mercado. Esta miopía consiste en que el titular de los datos venderá su información personal muy seguido y muy barato. Lo anterior, lo explica señalando: "En una transacción ordinaria, el consumidor valorará el dato a su valor marginal en términos de pérdida de privacidad. En cambio, un comerciante que vende el dato a un titular de banco de datos, valora el dato al o cerca del valor promedio como parte del perfil del titular de los datos. Porque, de acuerdo con nuestros supuestos, el valor promedio de un solo dato es mayor que el valor marginal del dato (recordando que el tratamiento de datos agrega valor al dato), el consumidor estará siempre dispuesto a vender sus datos al precio que el comerciante está dispuesto a pagar"[433]. De esta manera, este autor concluye certeramente que si los titulares de datos sufren de miopía respecto del valor de sus datos, pero los que efectúan tratamiento de datos no, y los datos son más valiosos dado el tratamiento efectuado, entonces habrá una sustancial sobre-divulgación de datos personales, incluso si los titulares de ellos se preocupan de su privacidad informacional.

[432] LAUDON, Keneth. op. cit. pág. 3.

En resumen, las fallas que se reconocen por la doctrina en el mercado de datos personales son las siguientes:

- Externalidad positiva: Las empresas reciben información personal que no han adquirido o comprado, a partir del conocimiento que adquieren de transacciones no dinerarias. Esta externalidad no sólo aplica al mercado de datos patrimoniales o financieros, sino que a todo el mercado desde que una determinada entidad tiene acceso a información personal no efectuando el costo respectivo, lo que usualmente ocurrirá en el mercado secundario de datos personales.
- Externalidad negativa: Se produce para los titulares de datos cuando deben asumir los costos del tratamiento de sus datos personales, sin haber intervenido en la respectiva transacción[434].
- Asimetría de información: La cual se produce tanto para los titulares de bancos de datos que no poseen toda la información personal que sí conocen los titulares de ella, como para los titulares de datos muchas veces no tienen información respecto del tratamiento que de sus datos se efectúa, como tampoco tienen las herramientas para valuar su información personal.

Se plantea frente a estas fallas del mercado de datos personales la necesidad de regularlo, presentándose a este respecto diversas fórmulas que revisaremos a continuación.

4.3. Regulación del mercado de datos personales

Las soluciones a las fallas que para algunos presenta el mercado de datos personales, pueden ser de doble naturaleza según quién sea el encargado de brindar la solución. Unos indican que son los propios actores de este mercado quienes puede remediar de una manera más eficiente las fallas que éste presenta a través de la autorregulación, y otros, establecen que es el Estado quien debe intervenir. De esta manera, existen dos grandes métodos para proteger la

[433] FROOMKIN, Michael. The Death of privacy? 2000. Stanford Law Review. 52: 1461-1543. pág. 1503.
[434] "El mayo uso de datos personales es en marketing directo por correo electrónico, teléfono, correo tradicional o en persona. En la medida que este marketing genera costos para los consumidores que aquellos que efectúan el marketing ignoran, éstos generan externalidades negativas". Hui, Kai-Lung y Png, Ivan. op.cit. pág. 25.

información personal. El primer método depende del mercado; la idea básica es que la reputación y las ventas de las empresas sufrirán si ellas vulneran la privacidad de los titulares de datos, que presentan interés en que su privacidad sea respetada, lo que hará que se autorregulen. El otro método depende del Estado. La idea básica es la aplicación de reglas legales obligatorias que disuadan a las instituciones de abusar de la privacidad informacional de las personas.

Como señala Peter Swire[435], teóricamente, el mercado o el estado podrían llevar a la protección óptima de la privacidad informacional. Si el mercado es suficiente fuerte, entonces las firmas encontrarán poco rentable utilizar información personal en formas que los individuos encuentren objetables. Si por otro lado, las reglas legales se definen correctamente, y la aplicación es suficiente efectiva, entonces las instituciones serán disuadidas de violar la privacidad de los titulares de datos. Sin embargo, en la práctica, como veremos a continuación, existen limitaciones importantes en la protección de la privacidad informacional, tanto si es el mercado el regulador de la industria, como si lo es el estado.

4.3.1. El mercado y la autorregulación

Bajo el modelo de mercado, los incentivos para proteger la privacidad son completamente económicos, no existe una norma legal en contra de las instituciones que revelan información personal respecto de los titulares de datos. Los titulares de datos pueden ser atraídos por una política fuerte de protección a la privacidad o bien, sentirse desincentivados por violaciones a la privacidad. Incluso, en algunos casos, la privacidad puede ser un ejemplo notable de marketing para inducir a consumidores a cambiarse de una compañía a otra[436]. Por otra parte, bajo este modelo se indica que las propias leyes de la oferta y la demanda regularán de la manera más eficiente el mercado de datos personales.

Jerry Kang resume la postura de aquellos que señalan que el propio mercado es el que da la solución más eficiente al problema del tratamiento de datos, este autor indica que “una vez que la información es producida, puede ser gobernada por las leyes de la oferta y la demanda. Desde este punto de vista, los intereses competitivos por la información personal serán

[435] SWIRE, Peter. op.cit. pág. 3.
[436] SWIRE, Peter. op.cit. pág. 2.

simplemente incorporados en su precio. De una parte, si el titular de los datos es un defensor de la privacidad o la información es particularmente sensible, entonces el titular de ella la valuará más que el que pretende efectuar tratamiento respecto de ella y le pagará a éste último para que no procese la información. De otra parte, si el individuo se preocupa poco de su privacidad, entonces el que efectúa tratamiento de datos valuará más la información personal y la procesará en todas las formas que impliquen una ganancia. Así, a través de las ofertas y contraofertas entre el titular de los datos y el que efectúa tratamiento de ellos, el mercado fijará el valor de los datos personales en su precio correcto, a la parte que los valúa más, en la medida en que esta parte desee y tenga la habilidad de pagar"[437]. Asimismo, se ha señalado a favor del mercado como regulador del propio mercado de datos personales, "que aunque las leyes de protección de datos crean un marco formal administrativo para la protección de los datos personales, ellas no incentivan a los individuos a tomar un papel activo en la protección de su propia información personal. Es por esto, que existen argumentos a favor de enfoques basados en el mercado, el cual crearía las condiciones para que los titulares de datos sean más proactivos en hacer las elecciones que se relacionan al intercambio de su información personal"[438].

Respecto a estos dos fundamentos que establecen que el mercado es el mejor y más eficiente regulador, observamos que, en primer lugar, si bien el ideal desde un punto de vista económico, es que los titulares de datos transen sus datos personales con aquellos que desean efectuar tratamiento de datos personales, la verdad es que lo anterior no ocurre debido fundamentalmente a las fallas que presenta este mercado y a los altos costos de transacción que existen hoy en día; y en segundo lugar, si bien compartimos la opinión que indica que las leyes sobre protección de datos personales no incentivan a los titulares a proteger activamente su información personal como tampoco a efectuar transacciones sobre ella, creemos que el anterior criterio no necesariamente lleva a la concluir que es el mercado el que mejor regulará el problema de la protección de datos personales, ya que puede argüirse que lo eficiente en este caso es una modificación legal.

---

[437] KANG, Jerry. Information privacy in cyberspace transactions. 1998. Stanford Law Review. 50: 1193-1294.pág. 1247.

[438] CAVOUKIAN, Anne. Privacy as fundamental human right vs. an economic right: an attempt of conciliation. 1999. [en línea] <http://www.ipc.on.ca/docs/pr-right.pdf> [consulta: 26 febrero 2006] 37p. pág.12.

De su parte, Daniel Solove[439] critica las soluciones al problema de la privacidad informacional que regulan el flujo de información personal basadas en un enfoque de mercado, de derechos de propiedad y de contratos. Indica que existen serias deficiencias en las soluciones de mercado y que el argumento que indica que el mercado está desde ya otorgando el nivel óptimo de privacidad, falla porque existen grandes desigualdades respecto al conocimiento (asimetría de información) y porque existe tratamiento de datos clandestino. El más fuerte argumento que invoca Daniel Solove en contra de la solución de mercado es aquel que señala que el mercado tiene dificultades en asignar el valor apropiado a la información personal como asimismo es difícil para el individuo dar un valor específico a sus datos personales, sobre todo, considera este autor, teniendo presente que el titular de la información personal no tiene conocimiento de los posibles usos futuros de sus datos personales. La dificultad de valorar los datos personales también se fundamenta para este autor en la posibilidad de cruzar datos personales, datos que son entregados por sus titulares en diferentes contextos y que en un comienzo no presentan mayores amenazas para la privacidad y que al ser cruzados efectivamente pueden vulnerarla. Indica además como argumento, que la posibilidad que los titulares de datos negocien en condiciones equitativas y justas con aquellas empresas o entidades que efectúan tratamiento de datos es difícil, debido fundamentalmente a la asimetría de información que existe entre las partes. Para este autor, el problema con el tratamiento de datos no es que aquellos que lo realizan no compensen a las personas por el apropiado valor de su información personal, sino que el verdadero problema es que las personas pierden el control, pierden el conocimiento acerca de cómo será usada su información personal en el futuro, y pierden la participación en este proceso.

Como decíamos en un comienzo, la principal forma en la que actúa el mercado en tanto mecanismo regulador de la industria de datos personales, es la autorregulación, es decir, el establecimiento voluntario por parte de los actores de este mercado –esto es, aquellos que efectúan tratamiento de datos personales- de normas y parámetros que regulen su actividad, sometiéndose a ellas, sin que exista, en todo caso, una facultad externa que exija su cumplimiento, de manera que el cumplimiento de estas normas autorregulatorias queda al arbitrio de los propios sujetos que las han creado. Sin embargo, para algunos la autorregulación

[439] SOLOVE, Daniel. 2001. Privacy and power: Computer databases and metaphors for information privacy. Stanford Law Review. 53: 1393-1462. pág. 1445.

es raramente voluntaria ya que ocurre generalmente sólo bajo la amenaza de la regulación del estado, y puede, por lo tanto, ser considerada como una variante de la regulación directa del estado[440].

Lawrence Lessig[441] critica este modelo, señalando que una condición necesaria para su éxito es que la comunidad encargada de aplicar las normas autorregulatorias, en este caso, las empresas e instituciones, incluya a todos aquellos que habrán de soportar el costo de la regulación de la conducta. Sin embargo, tales costos –los de la privacidad- recaen sobre los titulares de datos y no sobre las empresas e instituciones, y los usuarios, en la actualidad, no forman parte de la comunidad que establece las normas autorregulatorias.

En nuestro ámbito, Iñigo de la Maza también cuestiona este modelo señalando que aun cuando la protección de la privacidad beneficia tanto a productores como a consumidores, del lado de la oferta, tiende a producirse una situación similar a la presentada en el dilema del prisionero[442], indica este autor: "Aun cuando las empresas, como conjunto, obtendrían mayores beneficios si protegieran la privacidad de los usuarios, individualmente consideradas maximizan sus utilidades vulnerando el derecho a la privacidad de los usuarios". Es decir, las empresas no se autorregulan en materia de privacidad ya que no se sienten incentivadas a hacerlo.

Por otra parte, encontramos autores que defienden este mecanismo de regulación, en oposición a una regulación estatal, ya para ellos el mercado visiblemente responde a los problemas de privacidad de variada forma. "En primer lugar, las empresas que violan las expectativas de los consumidores acerca de su privacidad, enfrentan una pérdida de reputación, que se cristaliza en pérdidas en el mercado. Los efectos en la reputación son importantes; la evidencia muestra que cuando las empresas hacen algo que es percibido como perjudicial, su reputación se ve disminuida en los consumidores, las empresas sufren una sustancial pérdida de su valor. Cuando los empresarios usan la información personal de maneras que los consumidores no quieren, rápidamente éstos dan cuenta de ello, y las empresas se ven forzadas a parar. De esta manera, las empresas tienen un fuerte incentivo en orden a evitar políticas de privacidad que

[440] NOAM, Eli. op.cit. pág. 6.
[441] LESSIG, Lawrence. 2001. El código y otras leyes del ciberespacio. Madrid, Taurus. 544p. pág. 294.

ofendan o no agraden a los consumidores. En segundo lugar, las normas autorregulatorias definidas y fiscalizadas por terceras partes (consorcio, operadores de Internet), son un importante mecanismo para provee información a los consumidores acerca de las políticas de privacidad de las empresas. Existe evidencia que la autorregulación en Estados Unidos, funciona mejor que los estándares obligatorios adoptados por la Unión Europea. El 62% de los sitios web norteamericanos tienen políticas de privacidad, en cambio el porcentaje en la Unión Europea es de 32%. De manera que la voluntaria autorregulación provee mayor protección a la privacidad que la obligatoria regulación impuesta por los gobiernos. Por último, numerosa nueva tecnología, como por ejemplo la navegación anónima en Internet y el control de *cookies*, está disponible para los consumidores que se preocupan de su privacidad, ellos pueden usar estos servicios, algunos gratuitos, para proteger su información *on-line"*[443].

Un buen ejemplo en Chile en materia autorregulatoria, lo da el "Código de Buenas Prácticas en Internet" creado por la Cámara de Comercio de Santiago el cual tiene por objeto "regular las relaciones comerciales en Internet entre proveedores y consumidores, garantizando la protección al consumidor mediante la Ley 19.496 y la protección a la vida privada a través de la Ley 19.628"[444], dedica un capítulo especial a la privacidad del consumidor y la seguridad de sus datos personales, estableciendo como principio general que el proveedor en línea deberá adoptar y cumplir con una política de privacidad sobre el uso y protección de los datos personales que recolecta del consumidor, debiendo el consumidor en forma previa a la recogida de sus datos personales aceptar tal política. Finalmente, uno de los aspectos más interesantes de este Código es que establece que su aceptación es un requisito esencial para acceder al sello de confianza de la Cámara de Comercio de Santiago, y su cumplimiento una condición para conservarlo, lo que claramente incentiva a su adscripción y acatamiento. No obstante lo anterior, en entrevista con la funcionaria encargada de la implementación de este Código[445], observamos que en la práctica la cantidad de empresas que han adscrito al sistema es mínima; sólo mercadolibre y Paris. Lo anterior, debido al alto valor que las empresas señalan tiene la auditoría que permite tener el sello de confianza, (90 Unidades de Fomento). Se demuestra así, que en el

---

[442] Para una explicación del dilema del prisionero, ver. COOTER, Robert y ULEN, Thomas. Derecho y economía. 1ª reimpresión. 1999. México D.F., Fondo de Cultura Económica. pág. 55.
[443] RUBIN, Paul y LENARD, Thomas. op. cit. pág. 12.
[444] CAMARA DE COMERCIO DE SANTIAGO. Código de buenas prácticas. [en línea] <http://www.ccs.cl/html/codigo_buenas_practicas/inicio-cbp.htm> [consulta: 1 marzo 2006].
[445] Entrevista efectuada con fecha 30 de marzo de 2006 a doña Cossette Gutiérrez.

análisis costo-beneficio que efectúan las empresas el ítem “privacidad informacional” no es prioritario.

4.3.2. El Estado

Si el Estado interviene, es porque el mercado es en gran parte o enteramente ineficaz en proteger la privacidad informacional de los individuos. Las reglas sobre protección de datos personales son definidas por leyes, por regulación de agencias estatales, o por decisión de los tribunales, dependiendo del ordenamiento jurídico de que se trate, pudiéndose, por supuesto, encontrar una, dos o todas estas vías de protección actuando en conjunto. En este sistema, los afectados pueden demandar solicitando la aplicación de las reglas sobre protección de datos y existirá compensación cuando el individuo cuya privacidad es violada es indemnizado por tal violación, en cambio en un sistema que permite que los datos personales sean transados *ex - ante*, la compensación por la utilización de los datos personales, no sólo se produce cuando el tratamiento de la información es indebido o ilegal, produciéndose la violación del derecho, sino que en todo caso[446].

Se ha señalado por algunos autores que para estar ciertos sobre la necesidad de una regulación legislativa en el ámbito del tratamiento de datos personales, es necesario responder a ciertas cuestiones de política pública económica: En primer lugar, se debe establecer si existen fallas en el mercado de la información personal, luego, si éstas existen, verificar si afectan negativamente a los titulares de datos, además, se debe tener cierta claridad en cuanto a que estas fallas de mercado pueden ser solucionadas a través de la regulación legal, y por último, si los beneficios de la regulación exceden los costos de imponerla[447].

De esta manera y desde un punto de vista económico, la regulación del mercado de la información personal se debe efectuar sólo si el mercado no está funcionando apropiadamente. Una falla de mercado en este contexto implica que las preferencias de los consumidores sobre la cantidad y uso de su información no está siendo transmitida y recibida en forma adecuada. Si el mercado funciona bien, no se debe regular, ya que tal regulación producirá distorsiones

[446] Volveremos sobre las compensaciones en el próximo capítulo IV, al momento de analizar el modelo de Mercado de datos que se propone en esta tesis.

indeseables. Señalan estos autores que hay implícitas en algunas propuestas de regulación supuestos de fallas de mercado debido a que se estaría produciendo, diseminando y usando información en forma excesiva, de manera que el bienestar económico se lograría si las fallas del mercado son corregidas y la correcta cantidad de información es producida. Sin embargo, para estos autores lo anterior no es correcto, porque de una parte no existen evidencias que este supuesto exceso de información perjudique al titular de ella y porque, de otra parte, los mercados funcionan mejor con más información, ya que al existir más información el costo de ella baja, los participantes del mercado pueden adquirir más información, y, consecuentemente, pueden tomar mejores decisiones. Desde que los agentes del mercado por aplicación de los principios generales de la economía, se benefician con más información, cualquier política que reduzca la cantidad de ella, disminuirá la eficiencia, y se producirán efectos económicos negativos[448].

La posición anterior se ve un tanto mitigada respecto a ciertos tipos de datos personales, respecto de los cuales estos mismos autores reconocen: Los consumidores sólo actúan en orden a sus propios intereses. Las empresas que compiten por obtener más consumidores, deberían hacer sólo cosas que a los consumidores les guste. En este estado de cosas no se necesita regulación, sin embargo, los mercados no siempre funcionan perfectamente, ya que existen fallas de mercado que pueden conducir a malas elecciones económicas, esto es, elecciones que, en balance, fallan en maximizar el bienestar económico. Por todas estas razones, los gobiernos pueden y regulan la recolección y uso de información personal por empresas privadas. Hasta el día de hoy, esa regulación generalmente se ha enfocado en áreas en donde el perjuicio al consumidor es potencialmente grande, incluyendo datos de salud, información sobre finanzas personales, e información relacionada con niños[449]. En cada una de estas instancias, los titulares de datos están en una relativa posición débil para retener su información o las consecuencias del mal uso de su información personal es potencialmente grande, o ambas. En estas áreas, en otras palabras, el poder del mercado para proteger a los titulares de datos y disciplinar a las empresas que les causan perjuicio es bajo.

En este último sentido se ha indicado que “la finalidad de las políticas que pretenden

---

[447] RUBIN, Paul y LENARD, Thomas. op. cit. pág. 9.
[448] RUBIN, Paul y LENARD, Thomas op. cit. pág. 9-10.
[449] Estos autores, se refieren exclusivamente a la legislación dictada en estas materias en Estados Unidos. Para ver más información sobre esta materia.

perfeccionar el mercado de los datos personales debe ser reformar las fallas que este mercado presenta para reflejar más completamente los distintos valores que los individuos asignan a sus datos personales. Una vez que el mercado internalice estas preferencias, se producirá un aumento del bienestar social. Sin embargo, se debe señalar que desde una perspectiva económica es generalmente indiferente si algún excedente resultante de este aumento en el bienestar social se acumula a favor de los que efectúan tratamiento de datos o a favor de los titulares de ellos[450]. Las políticas de perfeccionamiento del mercado de datos personales requerirán, como mínimo, remover o al menos reducir la asimetría de información entre los recolectores de datos y los titulares de ellos"[451].

Los detractores de una regulación estatal para el tratamiento de datos personales fundamentan su oposición básicamente en que tal regulación generaría costos excesivos e ineficientes para este mercado. Así se ha indicado que "regular el mercado de la información personal puede traer costos. Si la información acerca de los consumidores se vuelve menos disponible y más cara, los vendedores pueden usar menos de ella y utilizar menos el *marketing to-one* o dirigido, de manera que los mensajes publicitarios pueden llegar a consumidores que no corresponden. Los consumidores pueden recibir más información no deseada, y como resultado, poner menos atención a la información que reciben. Esto puede aumentar el costo de comunicar esta información a los consumidores y el costo de los consumidores de obtener información. La pérdida de bienestar puede ser significativa ya que se pueden crear fallas de mercado que no existían"[452]. De otra parte indican que "la regulación puede tener negativos efectos para la entrada al mercado de nuevos actores, es decir, crear barreras de entrada debido al costo que genera el establecimiento de ciertas obligaciones, como la de notificar, de esta manera las empresas pequeñas tendrán una barrera de entrada al mercado, produciéndose, además como efecto secundario que esta regulación se constituye como una fuente de protección a las grandes firmas establecidas"[453]. Respecto de los anteriores argumentos, cabe indicar que el primero si bien es razonable desde un punto de vista económico, es restringido en cuanto a su aplicación ya que sólo se refiere a un tipo de datos personales: los datos con fines de marketing. El segundo

[450] Lo anterior desde un punto de vista de eficiencia paretiano.
[451] SCHWARTZ, Paul. op. cit. pág. 2082.
[452] RUBIN, Paul y LENARD, Thomas. op. cit. pág. 13
[453] RUBIN, Paul y LENARD, Thomas. op. cit. pág. 16.

argumento es de importancia y de general aplicación, por lo que efectivamente debe tenerse presente en cualquier regulación legal que se efectúe en la materia.

Desde un punto de vista de costos de transacción, Julie Cohen resume la postura de aquellos que se oponen a la privacidad informacional, al señalar que "entregar crecientes derechos de propiedad al individuo sobre su información personal, implicará un aumento irracional de los costos de transacción, incluyendo los costos de la negociación y de hacer cumplir las normas de protección de datos, costos que, en definitiva, deberán ser asumidos por los consumidores. Incluso, asumiendo que una mayor protección de datos es deseable, en términos de dignidad, los costos sociales pueden ser muy grandes"[454].

En este mismo sentido, basado en la generación de costos de transacción derivados de una regulación estatal, se ha indicado que "la regulación de la privacidad informacional por parte del estado produce costos administrativos para el estado y costos para la industria. Los costos administrativos incluyen el gasto del estado en el diseño de las reglas de privacidad, la administración de las reglas, e imponer las reglas en casos particulares. Los costos pueden ser sustanciales. La industria contraerá una variedad de costos con la regulación estatal. Asimismo, si los funcionarios del gobierno son incompetentes, entonces los costos de la regulación probablemente serán mayores y los beneficios menores"[455].

En el ámbito europeo, se reconoce también que existen costos en la regulación normativa del tratamiento de datos personales, especialmente derivados del derecho de los titulares de datos a acceder y corregir la información que les concierne y que es tratada por otros. Así, se indica, que el ejercicio de estos derechos puede tener consecuencias costosas para una organización "la entrega de información a los titulares de datos a menudo se ve como uno de los requisitos más onerosos para aquellos que efectúan tratamiento de datos. Sin embargo, se reconoce que la extensión de esta carga varía substancialmente, dependiendo del tipo de negocio realizado por la organización. La evidencia muestra que mientras el costo de tratar las solicitudes de acceso o una queja pueden ser significativos cuando ocurren, la incidencia de tales pedidos es

[454] COHEN, Julie. op.cit. pág. 1388.
[455] SWIRE, Peter. op.cit. pág. 5.

generalmente baja, significando que para la mayoría de las organizaciones el impacto económico es también bajo"[456].

Partidario de una regulación estatal de la privacidad a través de la ley, es Iñigo de la Maza quien indica que tal legislación debiera ser minimalista, garantizando al menos el consentimiento real e informado por parte del usuario acerca del uso de sus datos personales y "redactada en términos de garantizar estas dos metas, la legislación capturaría aquella área en que el razonamiento económico y el jurídico convergen: la protección de las decisiones de los sujetos. En el primer caso por motivos de eficiencia y en el segundo, por motivos de autonomía" [457].

Concluimos en esta parte, que el estado debe intervenir desde una óptica económica, cuando existen fallas en el mercado de datos personales, situación que claramente se observa y se constata en la realidad, por lo menos en la realidad nacional en la cual se avizoran estas fallas, así se puede observar muy a *prima facie*, que existen externalidades que afectan al titular de los datos, ya que en muchas ocasiones éste debe asumir la mayoría o la totalidad de los costos de una operación que tiene por objeto sus datos personales y que se realiza entre el responsable o tenedor de los datos y un tercero. También podemos observar que existe un oligopolio legal en el mercado de los datos personales patrimoniales, en donde, la Cámara de Comercio de Santiago a través de su Boletín Comercial goza del referido oligopolio respecto de los datos personales patrimoniales. Asimismo, se presente asimetría severa de información, pues en la mayoría de los casos el titular de los datos, ni siquiera tiene conocimiento que sus datos están siendo tratados o comercializados por otros, como tampoco tiene conocimiento acerca de a quiénes se transfieren los datos, si éstos son exactos, reales, cuál fue la fuente de la información, etc. Desde la perspectiva del que efectúa el tratamiento de los datos, hay ocasiones en las que también está presente la asimetría informativa, pensemos en todas aquellas hipótesis en que el titular del banco de datos no posee información que sí tiene el titular de los datos y que conlleva que los datos personales que se transan en el mercado sean de mala calidad. Lo anterior se aplica de igual manera a los terceros adquirentes de la información. Finalmente, los datos o la información

[456] HARRIS, Paul. The European perspective: is data protection value for money? [en línea] <http://26konferencja.giodo.gov.pl/data/resources/HarrisR_paper.pdf> [consulta: 05 marzo 2006]. pág. 4.
[457] DE LA MAZA, Iñigo. op.cit. pág. 275.

que es objeto de este mercado, si bien no constituye un bien público puro, ya que es excluyente, en la mayoría de los casos, sí tiene como característica el consumo no rival, ya que la obtención de un determinado dato personal por parte de un sujeto, no deja menos de información o datos para cualquier otro consumidor.

Sin embargo, al momento de regular legislativamente se debe tener presente una correcta asignación de titularidades que propenda al libre y eficiente intercambio de datos personales, cuidando de asegurar la autonomía de los titulares de datos y con ella la privacidad informacional, asimismo, se tienen que tomar en consideración los eventuales costos que puede generar una normativa en la materia, de manera de evitar que la regulación se vuelva un remedio que en definitiva no cure la enfermedad.

4.4. Regulación opt-in v/s opt-out.

En el ámbito anglosajón se reconocen dos formas de regular normativamente el mercado de datos personales, el denominado *opt-out* y el *opt-in*[458]. Bajo el *opt-out*, el que efectúa tratamiento de datos puede hacerlo libremente en tanto el titular de los datos no diga lo contrario. Bajo el *opt-in*, el tratamiento de datos personales sólo es permitido en la medida en que exista una autorización o consentimiento previo por parte del titular de ellos. Algunos autores[459] señalan que esta decisión (*opt-out* o *opt-in*), no es una decisión que se deba tomar *a priori* a través de una normativa, ya que optar por una o por otra dependerá del específico tratamiento de datos que se efectúe, y de los intereses de los actores que efectúan tratamiento de datos y de los titulares de ellos[460]. De otra parte, agregan que hay evidencia que indica que la gran mayoría de los titulares de datos acepta la regla que se adopte[461]. Según estos autores los consumidores

[458] Todavía encontramos una tercera forma de regular este mercado a través de una norma legal. Jerry Kang plantea que hay dos opciones legales que la sociedad puede adoptar: a una la denomina "*plenary use*" y a la otra "*functionally necessary use*". En la primera opción, a menos que las partes acuerden otra cosa, el que efectúa tratamiento de datos, puede procesar o tratar datos personales de la manera que él quiera, en la segunda, a menos que las partes acuerden otra cosa, sólo puede procesar o tratar datos en la medida en que sea necesario para completar o ejecutar una transacción a partir de la cual la información personal fue originalmente extraída. KANG, Jerry. op.cit. pág. 1249.

[459] RUBIN, Paul y LENARD, Thomas. op. cit. pág. 73.

[460] Olvidan estos autores que puede optarse por un sistema híbrido que reconozca la existencia de un sistema general de reglas *opt-in* o bien *opt-out*, con ciertas excepciones respecto a determinados tratamientos de datos personales.

[461] Un testimonio de la *Federal Trade Comission* respecto de la experiencia de una empresa, indica que cuando la regla era *opt-in*, el 85% de los consumidores escogió no proveer su información personal. En contraste, el 95% escogió proveer sus datos personales cuando la regla era el *opt-out*.

aceptan la regla que exista, porque ellos de alguna u otra manera no consideran el tema muy importante. Pero, en realidad, es porque los costos de transacción asociados a tomar una decisión, que incluyen leer la política de privacidad y entender la naturaleza de la elección, no es menor. Esto es, los costos de transacción asociados con el proceso de *opt-out* y el *opt-in* no son insignificantes y éstos son asumidos, en última instancia por los propios consumidores. Si los costos de transacción son lo suficientemente bajos, los derechos legales se mueven hacia el uso más valioso. La asignación inicial del derecho no importa. Si los costos de transacción son significativos, es eficiente asignar el derecho a la parte que lo valúa más, o a la parte que puede comprarlo si los costos de transacción son menores. En este caso, la parte es el que efectúa tratamiento de datos. Esto implica que, si tiene que haber una regla esta debe ser el *opt-out*. Si la regla fuera *opt-in*, la información no fluiría a su uso más valioso.

La opinión anterior no es compartida por todos, algunos autores indican que históricamente el costo de obtener el consentimiento del titular de los datos previo al uso de su información personal era tan grande que era más eficiente asignar la propiedad de la información del titular al que efectuaba el tratamiento. Pero que actualmente la creciente eficiencia de las modernas tecnologías en el tratamiento de datos produce una gran reducción de estos costos. Las empresas, pueden ahora obtener y solicitar autorización a los titulares de los datos a menor costo que antes. Se distinguen y plantean dos modelos en el mercado de tratamiento de datos, el "control organizacional", que se caracteriza porque se le otorgan derechos de propiedad intelectual a las empresas sobre los bancos de datos que contienen la información personal; modelo que operaba en parte, porque el costo de obtener y aplicar reglas de *opt-out* o *opt-in* era simplemente muy alto. El segundo modelo es denominado "control individual" y se basa en que desde que la tecnología ha hecho más barato y fácil aplicar al tratamiento de datos controles como el *opt-out* o *opt-in*, se hace más económico y más efectivo, desde un punto de vista de los costos, transferir la propiedad y el control de los datos personales al único actor en el sistema que se presenta en todas las bases de datos: el titular de los datos personales[462].

[462] 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].
Paul Sholtz es de la misma opinión cuando indica -en base al teorema de Coase- que la existencia de bajos costos de transacción (permitidos por las nuevas tecnologías) implica que los titulares de datos deben tener derechos de propiedad sobre su propia información. SHOLTZ, Paul. op.cit. pág. 13. Jessica Litman, tiene la opinión contraria, para ella no tiene sentido señalar que los costos de transacción son bajos o que pronto lo serán, de manera que los individuos podrán alcanzar acuerdos

Otra autora, Loretta Nott, efectuando el análisis sólo respecto de los datos de naturaleza financiera, indica a este respecto que cuando existen externalidades, la teoría económica indica que una eficiente asignación puede ser alcanzada cuando los derechos de propiedad están bien definidos[463]. Las políticas públicas asignan el derecho de propiedad sobre la información financiera a través de la elección entre el *opt-in* y el *opt-out.* Bajo la opción *opt-out* las instituciones financieras tienen el derecho a compartir la información financiera que posee con sus afiliados. Los titulares de datos ejercerán el *opt-out* cuando el valor de su privacidad financiera exceda el valor producido por el intercambio de su información. En este caso, las instituciones financieras competitivas tendrían un incentivo por competir por esos titulares de datos ofreciendo compensarlos por el uso de su información financiera. En la opción *opt-in*, los consumidores efectivamente tienen el derecho de propiedad sobre su información financiera. En este caso, las instituciones financieras tendrán un incentivo a comprar esa información hasta el punto donde la ganancia económica se iguale al costo de compensar a los titulares de datos. De manera, que no importa cómo los derechos de propiedad han sido asignados, el mercado logrará la eficiencia. Por otra parte, esta autora indica que cuando existe información imperfecta, las instituciones financieras se benefician de ella y la eficiencia económica no se logra, ya que si los titulares de datos no conocen completamente el valor de mercado de su información financiera, no ejercerán el *opt-out* aun cuando tengan la posibilidad de hacerlo, y las instituciones financieras podrán recibir las ganancias económicas de intercambiar esa información sin pagar a los titulares su verdadero valor. Según esta autora, si hay información imperfecta las políticas públicas deben promover la opción *opt-in*, ya que si las instituciones financieras deben obtener el explícito consentimiento de sus clientes para tratar su información personal, entonces ellas tendrán un incentivo a ofrecer una compensación a sus clientes por el uso de esa información.

Esta autora indica que en las políticas públicas sobre esta materia (escoger entre *opt-in* u *opt-out*), se deben tener presentes el nivel de ganancia del uso de la información financiera y los costos de transacción. Respecto de lo primero, si los márgenes de ganancia son pequeños en el intercambio de información personal para las instituciones financieras, el modelo *opt-in* puede

---

individuales acerca del uso y divulgación de sus datos personales. LITMAN, Jessica. op. cit. pág. 1297.

[463] El término derechos de propiedad es usado por los economistas para representar la propiedad o control sobre un bien, y no debe ser interpretado como una definición legal de derecho de propiedad.

llevar a que el mercado de información financiera se derrumbe ya que el costo adicional que se requiere para compensar a los titulares de datos por el uso de su información financiera puede eliminar la ganancia económica de recolectar e intercambiar esta información y como resultado estas instituciones cesarán de intercambiar esta información, con ello, los titulares de datos ya no recibirán los beneficios de poder efectuar mejores elecciones de productos y servicios financieros. En este caso, el control efectivo de la información financiera será más eficiente si se opta por el modelo *opt-out.* En relación a los costos de transacción, éstos pueden existir tanto de parte de los titulares de datos, en términos de inconvenientes y tiempo, y para las instituciones financieras puede resultar costoso solicitar autorización de cada cliente para utilizar su información personal. Si estos costos son significativos, la teoría económica sugiere que una asignación eficiente es aquella que asigna el derecho a quien puede minimizar los costos. Si los costos de transacción son mayores para las instituciones financieras que para los titulares de datos, la teoría indica que el modelo *opt-out* es el más eficiente[464].

Para Paul Schwartz[465] la regla *opt-in* implica un avance frente a la regla del *opt-out*, debido a que un régimen *opt-in* mejora el funcionamiento del mercado de la información personal, ya que reduce los problemas de asimetría de la información al forzar al que efectúa tratamiento de datos a obtener el consentimiento del titular de los datos para poder adquirir, usar, y transferir su información[466].

E. Rose[467] señala que los partidarios de la privacidad proponen una legislación *opt-in* pero, ¿dónde están los incentivos para hacer cumplir estos derechos legales de los titulares de datos? La respuesta a esta pregunta la da la misma autora: imponer costos más altos a los que efectúan tratamiento de datos. Con esto, la opción *opt-in* puede bajar el valor de la información personal y disminuir el intercambio de información y con ello, la potencial violación de la privacidad. Los que efectúan tratamiento de datos no tendrán incentivo en cumplir esta legislación, por lo tanto, el gobierno tendrá que hacerlo a través de subvenciones a los que

[464] NOTT, Loretta. op. cit. pág. 7.
[465] SCHWARTZ, Paul. op. cit. pág. 2103.
[466] Este mismo autor indica que una de las objeciones posibles al modelo de *opt-in*, es aquella que señala que este sistema crea un desincentivo para las empresas, que las disuadirá de efectuar transacciones sobre información personal, en un análisis costo-beneficio, ya que la empresa no efectuará este tipo de transacciones si requerir la autorización del titular de los datos es más costoso que los beneficios que le produce realizar el referido tratamiento.
[467] ROSE, Ellen. op.cit. pág. 3.

efectúan tratamiento de datos o bien, imponiendo impuestos a los titulares de datos con el objeto de que paguen los costos de hacer cumplir la legislación. Pero, ¿estarán los titulares de datos dispuestos a pagar por la protección de su privacidad?

Para responder esta pregunta la autora analizó la respuesta de 459 neocelandeses a una encuesta realizada con el objeto de estimar el valor económico que los titulares de datos asignan a un hipotético cambio a las leyes de protección de datos en orden a entregar a los titulares de datos una mayor fuerza para hacer cumplir los derechos de propiedad sobre su información personal.

Se preguntó directamente a los individuos por su disposición a pagar: ¿sujeto a su restricción monetaria actual, estaría dispuesto a pagar "$X" por año en mayores impuestos para fortalecer la protección de sus datos personales por medio de la ley? (si o no). Sólo un 47,5% de los encuestados estaba dispuesto a pagar. Esto implica que una porción significativa de neocelandeses valora la protección de la legislación *opt-in*, quizás debido a una mayor valoración de estos individuos a la existencia de privacidad y una falta de confianza en las organizaciones para imponer las protecciones. En cambio, un 52,5% no estaba dispuesto a pagar, estos individuos podrían ser considerados "*free riders*".

De lo señalado por Richard Posner[468] podemos concluir que él resulta ser partidario del *opt-out*, aun mucho antes que el debate sobre estas materias se efectuara en los términos que se están revisando, Posner indica que: "Si nosotros creemos que esas listas , generalmente valen más para los compradores que el valor que los suscriptores le otorgan a ser protegidos de eventuales solicitudes no deseadas, nosotros debemos asignar el derecho de propiedad a la revista; y la ley lo hace".

Como podemos observar existen fuertes argumentos para escoger tanto la opción *opt-in* como el *opt-out*, al momento de regular normativamente el mercado de datos personales. Creemos, sin embargo, que si bien en una primera instancia y como regla general se ha de optar por una de estas alternativas, se debe considerar en la legislación excepciones a la regla

[468] POSNER, Richard. 1978. The right of privacy. Georgia Law Review 12: 393-422.

escogida, conforme según se trate de distintos tipos de datos personales, de manera de recoger de ambas opciones aquellos aspectos que las hacen eficientes.

4.5. Asignación de titularidades

En el presente acápite revisaremos un tema íntimamente vinculado al anterior, ya que cuando hablamos de optar por una legislación *opt-in* u *opt-out* lo que estamos haciendo en gran medida es referirnos a la asignación de titularidades o de derechos de propiedad, esto es, en términos simples: ante un conflicto de intereses determinar a qué sujeto otorgamos la titularidad respecto del derecho que está en disputa. En el caso que nos ocupa, la literatura consultada se ha pronunciado de diversas maneras, estableciendo que los derechos deben ser asignados al titular de los datos personales, como también que lo han de ser a aquél que efectúa el tratamiento de los datos. Cabe indicar, que siempre los fundamentos para optar por una u otra opción son de naturaleza económica, ya que buscan lograr la eficiencia en el mercado de datos personales, utilizando, la gran mayoría de las veces el teorema de Coase.

Como indica E. Rose, los partidarios de la privacidad informacional señalan que su violación es un costo social derivado del aumento en el comercio de los datos personales que se ha producido por los avances en tecnologías de administración de información e Internet. De su parte, los usuarios de este tipo de datos señalan que los beneficios del intercambio libre de información son entregados a los propios titulares de datos y que estos beneficios pesan más que potenciales infracciones a la privacidad informacional. Un asunto central es debatir sobre quién posee y quién controla la información personal, es decir, discutir sobre la asignación de titularidades[469].

Paul Sholtz[470] aplicando el teorema de Coase, indica que si es claro que existen significantes fallas de mercado en la manera en que las empresas recogen y usan la información personal y que la autorregulación no está funcionando eficientemente, Coase entrega una alternativa que debe ser considerada: la redefinición y asignación de los derechos de propiedad. A lo anterior agrega que se ha de tener en especial consideración la naturaleza recíproca del

[469] ROSE, Ellen. op.cit. pág. 1.
[470] SHOLTZ, Paul. op.cit. pág. 8-9.

costo social. Aplicando lo dicho a la privacidad informacional, este autor entrega un importante antecedente; señala que el foco de la discusión en estas materias ha sido identificar las maneras en que los que efectúan tratamiento de datos perjudican o dañan a sus titulares, de forma que el debate ha recaído en cómo impedir que los que recolectan información personal perjudiquen a las personas que proveen esa información, poniendo poca atención en el hecho que los problemas de privacidad sólo pueden ser creados por una decisión conjunta entre titulares y los que realizan tratamiento de datos personales, lo cual es importante porque implica que asignar responsabilidad a una cualquiera de las partes es correcta en términos de eficiencia, si la parte a la cual se considera responsable puede compensar la externalidad al menor costo posible. La afirmación que efectúa Sholtz hace sentido en nuestro sistema legal, ya que en éste los perjuicios producidos por un tratamiento indebido de datos se resuelven por reglas de responsabilidad. Coincidimos con este autor cuando señala que atribuir responsabilidad al que efectúa el tratamiento indebido de datos, es eficiente desde un punto de vista Coasiano, si aquél puede resolver los problemas de privacidad que genera su accionar a menor costo que los titulares de datos. Sin embargo, agrega en su razocinio el elemento tecnológico, el cual cambia la regla tradicional anterior, ya que señala que la tecnología existente en la actualidad permite a los titulares de datos ejercer un gran control sobre su información personal, lo que hace que la solución legal tradicional -asignar la responsabilidad al que efectúa el tratamiento- sea obsoleta, lo anterior siempre y cuando, previene, los derechos de propiedad estén correctamente asignados. En este sentido, expone una interesante y diferente mirada a la aplicación del teorema de Coase a la privacidad informacional, al indicar que algunos autores se equivocan cuando señalan que los derechos de propiedad deben asignarse a la parte que más valúa los datos personales y que ello implicaría que los titulares de datos tienen el “derecho” a “vender” su privacidad. Para este autor, ambas partes en un intercambio comercial valúan la información personal valiosamente (por distintas razones), y que el que realmente debe ser el titular de los derechos de propiedad, es aquella parte que no venderá su derecho de propiedad una vez establecido. Indica que el real problema del intercambio de información personal son las externalidades y que el teorema de Coase lo que señala es que el derecho de propiedad debe ser asignado a la parte que puede resolver estas externalidades a un menor costo y no a la parte que valúa más la información personal, y que esta parte en el estado actual de la tecnología son los

titulares de los datos personales y que por ende a ellos se les deben asignar los derechos de propiedad sobre su información[471].

Con distintos fundamentos económicos, Kenneth Laudon[472] también se muestra partidario de asignar los derechos de propiedad a los titulares de los datos personales, así señala que el problema de la privacidad informacional no sólo deriva de la utilización casi masiva de las nuevas tecnologías, sino que también se produce porque existen fallas en el mercado de datos personales derivados de una pobre asignación de derechos de propiedad, señalando que esta se corresponde a aquella legislación que entrega los derechos de propiedad a aquél que efectúa tratamiento de datos y no al individuo al cual se refieren los datos. Continúa indicando que como consecuencia de lo anterior, los titulares de datos no pueden participar del mercado de datos personales, y no reciben la adecuada compensación por el uso de su información personal, de manera tal que el precio de la información personal es tan bajo, que las industrias se vuelven ineficientes en su uso, el precio es bajo porque el precio de la información personal no refleja el real costo social de reproducir información personal. Indica que estas terceras personas que compran y venden información pueden imponer costos a los titulares de datos, sin que éstos se vean directamente envueltos en la transacción, es decir, existe una externalidad negativa.

Por otra parte, encontramos autores que indican que es eficiente asignar los derechos de propiedad a los titulares de los bancos de datos, así Alfredo Bullard[473] se pronuncia sobre la definición legal que se adopte en materia de privacidad y los costos de transacción, señalando que tal definición "tendrá una influencia directa en los costos de transacción que se den en una sociedad. La elevación de estos costos de transacción relativizarán la capacidad del mercado de internalizar o corregir externalidades por medio de las decisiones de los agentes económicos. La asignación de costos no nos conduciría entonces, necesariamente, a una solución eficiente. En resumidas cuentas la definición e importancia que la sociedad dé al derecho a la privacidad influirá en cómo funcionarán los mercados y en cuánto bienestar pueden generar éstos." En este sentido, cree que al reducir los niveles de información personal disponibles socialmente el control de la información por parte de quien alega la vulneración de su privacidad puede conducir a elevar los costos de transacción y con ello a que se generen externalidades donde

[471] SHOLTZ, Paul. op. cit. pág. 16.
[472] LAUDON, Keneth. op. cit. pág. 1.

parte de los costos de la actividad de las personas no sean asumidos por quienes los generan. Así el costo de la incertidumbre generada por la falta de información considerada privada afecta a todos y no sólo a aquellos beneficiados por mantener oculta cierta información[474]. En base a lo anterior, Alfredo Bullard se inclina por no establecer la privacidad de la información personal, respecto a este punto señala "lo que interesa es preservar un derecho de exclusividad pero sin permitir que el mismo pueda ser utilizado para generar externalidades a terceros por la vía de incrementar los costos de transacción a niveles tales que ya no sea posible que el mercado haga una asignación correcta de recursos escasos. Así información como el historial delictivo, los antecedentes de crédito o la historia laboral deberían estar a disposición de las personas. No queda claro en tales casos cuál es el beneficio que genera la reserva de ese tipo de información distinto a permitir una representación inexacta de la imagen de una persona, lo que induce a que se cometan errores al juzgarse sus cualidades y capacidades." Establece que, en todo caso, esta premisa requiere que la información disponible sobre estos aspectos sea veraz y exacta. De lo contrario se elevarían los costos de transacción por la mala información existente, con un efecto incluso peor que el omitir información en el mercado.

Para E. Rose[475] una alternativa de mercado es la reasignación de derechos de propiedad a la parte que pueda mejorar la situación con los menores costos de transacción en términos de negociar y suscribir un contrato para un cambio beneficioso. Sin embargo, reconoce que es actualmente difícil que los titulares de datos contraten con los que efectúan tratamiento de sus datos debido a la dificultad de suscribir y hacer cumplir dichos contratos lo que junto con la asimetría de información constituyen impedimentos significativos para el establecimiento de un mercado puro de derechos económicos de propiedad. Por último, señala esta autora que debido a los altos costos impuestos a los titulares de datos para controlar y buscar mejores contratos, los que efectúan tratamiento de información personal son los que evitan los costos a menor precio (*least cost avoiders*) y retienen la mayoría de los derechos económicos de propiedad sobre el tratamiento de información personal[476].

---

[473] BULLARD, Alfredo. op.cit. pág. 24.
[474] BULLARD, Alfredo. op.cit. pág. 25.
[475] ROSE, Ellen. op.cit. pág. 3.
[476] Ibídem.

Charles Kahn, James McAndrews y William Roberts en su artículo "A Theory of transactions privacy"[477] efectúan un análisis de la necesidad o no de asignar titularidades en el ámbito de la privacidad informacional. De esta manera, aplicando la lógica de Coase, señalan que si existe suficiente flexibilidad para los contratos, no serían necesarias rigurosas leyes protectoras de datos para lograr eficiencia en la ocultación o revelación de información. Sin embargo, para estos autores existen razones importantes por las cuales se puede esperar que la flexibilidad contractual se encuentre limitada en el contexto de transacciones en la privacidad informacional. Primero, existen limitaciones naturales como la propia incapacidad de comprometerse a no utilizar información una vez adquirida. En segundo lugar, la utilidad de la información adquirida está probablemente atada a una gran cantidad de inversiones efectuadas por las partes que transan, de manera que los contratos probablemente serán difíciles de hacerse cumplir por las mismas partes. Consecuentemente, la elección de derechos de propiedad tendrá implicancias en el bienestar de los participantes en estos mercados. Por otro lado, se puede llegar a una asignación ineficiente en relación a la liberación de información cuando los contratos son "limitados", y por lo tanto debería existir una intervención al mercado.

Por ejemplo, consideremos una transacción entre un consumidor A y una firma B, además, existe un intruso C quien se beneficiará del conocimiento de la transacción entre A y B. Revelar la transacción a C afecta la utilidad de A y B. En este ejemplo sencillo, revelar la transacción es socialmente deseable si y sólo si la ganancia resultante en la utilidad de C pesa más que cualquier pérdida de utilidad sufrida por A o B. Para hacer el ejemplo más concreto, suponga que un consumidor desea comprar un equipo de sonido de alta calidad a algún vendedor. El conocimiento de esta compra puede ser valioso a una variedad de terceros. Por ejemplo, vendedores que venden bienes complementarios al bien inicial (vendedores de CD), compañías que inspeccionan la satisfacción del consumidor, compañías interesadas en conocer la historia de crédito del consumidor y ladrones especializados en equipos de música.

En algunos casos, el consumidor estará ansioso en que terceros aprendan acerca de la compra, como en el caso del vendedor de CD. En cambio, el consumidor prefiere claramente que el ladrón no sea informado de la transacción. Respecto de otros casos, como por ejemplo, compañías interesadas en conocer la historia de crédito, puede ser poco claro si el consumidor

[477] CHARLES KAHN "et al". op.cit. pág. 1.

apoya la idea o no de la liberación de información. Del mismo modo, existen también beneficios positivos o negativos para la firma cuando terceros aprenden acerca de un consumidor.

En el contexto del ejemplo, el primer mejor resultado se obtendría claramente en un ambiente cooperativo en el que A, B, y C entren libremente a un acuerdo multilateral con respecto a la liberación de información. ¿Pero qué se puede decir acerca de ambientes no cooperativos en los que ni A ni C saben de la existencia del otro antes de la transacción? Si el vendedor B posee el derecho de revelar la compra de A a C, entonces para inducir a A ha hacer una compra, B debe compensar suficientemente a A por la molestia de revelar la transacción. O, si el consumidor A posee el derecho de revelar la transacción, B y C tendrían que compensar a A antes que cediera este derecho. En ambos casos, se obtendría la mejor asignación con una suficiente negociación.

Las conclusiones de este modelo son consecuentes con la teoría de Coase, en donde al negociar con suficiente flexibilidad contractual entre las partes y derechos iniciales claramente definidos llevará al mejor resultado social. Sin embargo, el estado actual de la ley no siempre asigna los derechos sin ambigüedades. Por lo tanto, en muchos casos, la asignación inicial de derechos afecta el resultado, y puede, consecuentemente llevar a una solución ineficiente.

Como señala Hal varian, creemos que una adecuada manera de resolver los problemas que presenta el tratamiento de datos, es determinar una buena asignación de derechos, permitiendo y facilitando, en todo caso, a los titulares de datos comerciar con ellos, si así lo desean. Hemos verificado que dada las fallas del mercado y la existencia de significativos costos de transacción en las eventuales transacciones que se efectúen entre el titular de los datos y aquellos que se encuentran interesados en efectuar tratamiento con tales datos, sí es importante la asignación inicial de derechos que se efectúe por la ley, de manera que conforme los postulados de Coase los derechos se deben asignar allí donde los costos se minimicen y a la parte que valúe más el derecho. Finalmente, se ha de tener presente en el análisis tanto los costos de transacción del titular de los datos como los de aquél que pretende adquirirlos o que efectúa tratamiento de datos personales.

4.6. La privacidad informacional como propiedad

La propuesta que ha generado mayores comentarios recientemente, es la idea que la privacidad puede ser tratada como un derecho de propiedad. Las personas son dueñas de la información sobre ellas mismas, y, como dueñas, están facultados para controlar qué se hace con ella[478]. Esta idea se encuentra íntimamente ligada con el análisis económico que efectúan algunos economistas estadounidenses sobre la privacidad informacional y el mercado de datos personales. Así por ejemplo, Kenneth Laudon[479] señala que la crisis actual en materia de privacidad informacional existe porque hay fallas en el mercado, las cuales, podrían ser corregidas tratando la información personal como propiedad, para luego darle un precio que refleje su valor; Hal Varian[480] analiza la privacidad informacional de los consumidores como un derecho de propiedad sobre la información privada, en orden a explorar la posibilidad de que los consumidores tenga control sobre el uso de sus datos personales; Paul Sholtz[481] señala que derechos de propiedad sobre la información personal que se intercambia bajo contratos en el curso de una transacción comercial puede resolver muchos problemas actuales y futuros en relación a la privacidad informacional, desde que se reconoce el rol del titular de los datos como el que evita la externalidad al menor costo.

En general, hemos podido observar que en aquellos casos en que se reconoce la existencia de fallas en el mercado de datos personales, es la propietarización de la privacidad informacional la solución planteada por los autores, así por ejemplo, Paul Schwartz[482] reconoce que muchos entendidos creen que el mercado de la privacidad no funciona bien debido a la existencia de fallas en el mercado, pero indica que la probabilidad que estas fallas se corrijan por sí mismas es muy baja, de manera que se debe recurrir a la propietarización de la información personal.

Desde un punto de vista más cercano al derecho, Ann Couvakian indica que la propiedad se ha descrito como una relación legal entre una persona y una cosa, en donde la cosa puede ser física o intelectual. Estos derechos incluyen el derecho de utilizar la propiedad como uno desea,

[478] LITMAN, Jessica. op. cit. pág. 1287.
[479] LAUDON, Keneth. op. cit.
[480] VARIAN, Hal. 1996. op.cit.
[481] SHOLTZ, Paul. op.cit. pág. 11.

de excluir a otros, de alterar su configuración, de gozar sus frutos y rentas, y por supuesto, de transferir la propiedad. Esta autora establece como fuente de la privacidad el derecho de propiedad, y en este sentido, señala que la propiedad es una fuerte herramienta en contra del poder estatal y las empresas, de manera, que por extensión, la privacidad como una directa extensión de la propiedad, puede proteger a los débiles en contra de los fuertes[483].

De su parte, Stan Karas[484] efectuando un análisis en el ámbito de la privacidad informacional de los consumidores, indica que el enfoque de la información como privacidad implica aceptar que los consumidores pueden vender, licenciar o negar su información a los que la requieran. Para este autor los beneficios de esta postura son dos: los consumidores recuperan el control sobre la distribución de su información personal y serán compensados por el uso de sus datos personales. Este autor no obstante reconocer que propietarizar la información personal es una solución al problema, no lo enmarca de una manera adecuada, ya que olvida las razones por las cuales se busca proteger este tipo de información.

La propietarización de la privacidad informacional también ha sido defendida por algunos profesores de derecho en Estados Unidos: Jerry Kang, explora un modelo de mercado de derechos de propiedad como una oportunidad para establecer reglas supletorias que puedan que puedan aumentar el control de los consumidores sobre su información personal[485]; Pamela Samuelson[486], indica que la propietarización de la información personal puede tomar ventaja del mercado de información personal existente y dar a los miembros del público algún control, del que actualmente carecen, sobre el tráfico de sus datos personales.

Pero no todos los autores consultados están contestes en que la propietarización de la privacidad informacional sea la solución a los problemas asociados a ella, algunos como Jessica Litman[487] vislumbran serios problemas en proponer un sistema de propietarización de la información personal, esta autora señala en primer lugar, que establecer derechos de propiedad

---

[482] SCHWARTZ, Paul. op.cit. pág. 2076.
[483] COUVAKIAN, Anne. op.cit. pág. 18.
[484] KARAS, Stan. Privacy, identity, databases: toward a new conception of the consumer privacy discourse. Stanford Technology Law Review. 2002. [en línea] http://stlr.stanford.edu/STLR/Working_Papers/02_Karas_1/ [consulta: 12 diciembre 2003]
[485] KANG, Jerry. op. cit.
[486] SAMUELSON, Pamela. Privacy as intellectual property? 2000. Stanford Law Review 52: 1125-1171.

sobre cualquier tipo de información choca con la libertad de información, con la cual la sociedad norteamericana tiene un gran compromiso[488]. Asimismo, indica que cuando se reconocen derechos de propiedad sobre hechos, se adhiere a la idea que los hechos pueden ser apropiados y que su dueño se encuentra facultado para restringir el uso que de ese hecho se puede hacer, lo cual es inconsistente con la jurisprudencia actual en Estados Unidos sobre la primera enmienda constitucional.Agrega al fundamento constitucional como crítica a la propietarización uno que dice relación con el elemento alienabilidad intrínsico al derecho de propiedad. Señala que la razón de ser de la propiedad es la alienabilidad, que el propósito de las leyes de propiedad es prescribir las condiciones de su transferencia. Estas leyes le otorgan al propietario control sobre un ítem determinado y la habilidad de venderlo o licenciarlo. Este control (derecho de excluir) es análogo a diferentes tipos de control conferidos por distintos tipos de leyes, para esta autora no es necesario tratar un interés como propiedad en orden solamente a proteger este interés de una invasión, ya que esta protección es tradicional de la responsabilidad. Señala que si se considera algo como propiedad es para facilitar su transferencia, de manera que si no se pretende que ese algo se transfiera (porque lo que realmente se requiere es que no se invada)[489], entonces no se necesita tratarlo como propiedad. Luego esta autora critica la propietarización, pero sólo desde la óptica de aquél que efectúa tratamiento de datos, indica que dado que los datos personales son valuables, los que los tratan efectúan demandas de propietarización sobre la información personal que ellos compilan, basadas en el esfuerzo y la inversión que han efectuado para tener esa información. Si los que efectúan tratamiento de datos pueden demandar que los datos personales son de su propiedad, el valor de cada dato se incrementará porque el propietario estará facultado para controlarlo en forma exclusiva, lo que a su turno, aumenta los incentivos para recolectar la mayor cantidad de datos personales posible[490].

Julie Cohen[491] indica que existe una correlación negativa entre la propiedad sobre los datos personales y el nivel resultante de privacidad, ya que reconocer derechos de propiedad

---

[487] LITMAN, Jessica. op. cit. pág. 1294.
[488] Cabe hacer notar que este argumento es de difícil aplicación en nuestro ámbito, sobre todo, en relación con la interpretación que de este derecho han efectuado los Tribunales de Justicia, los cuales tienden a proteger en los conflictos entre el derecho a la privacidad y el derecho a la libertad de información, al primero. Ver Análisis de la jurisprudencia de los Tribunales Superiores de Justicia, en materia de libertades constitucionales, desde el año 1980 hasta el año 200 y su relación con la contingencia política del país. Revista Chilena de Informática Jurídica, Jurimetría. 2002. Santiago, Chile. 1.
[489] El paréntesis es nuestro.
[490] LITMAN, Jessica. op. cit. pág. 1299-1300.

sobre los datos personales, producirá más comercio y menos, y no más privacidad. Para ella, las fallas del mercado harán que la gente comercie en demasía sus datos personales propietarizados y por esta razón, se erosionarán los niveles de privacidad existentes. No obstante lo anterior, cree que definiendo estos derechos de propiedad, en cambio, en términos de carga, en la línea general que sugiere los derechos de propiedad intelectual, ofrece la posibilidad de entregar al individuo el control sobre su privacidad[492].

En el ámbito latinoamericano, se ha discutido también respecto de la posible existencia de una relación entre el derecho de propiedad y los datos personales, sin embargo, las disquisiciones no llegan a pronunciarse directamente sobre la conveniencia o no de adoptar como modelo el de la propietarización de la privacidad informacional. No obstante lo anterior, creemos de relevancia revisar lo señalado por algunos autores respecto de esta importante aspecto.

Antonio Ruiz[493] expone que los datos de índole personal son propiedad, ante todo, de su titular y, subsidiariamente, de los poderes públicos y de las personas o instituciones privadas que posean el consentimiento expreso o tácito del titular para ser tratados, transferidos y/o administrados. Distingue este autor entre los datos de titularidad pública y privada, respecto de los primeros señala que las instituciones públicas son propietarias de los datos de índole personal por consentimiento expreso o tácito manifestado por el padre o tutor, naciendo la propiedad cuando los datos son consignados en el Registro Civil, todo ello por imperativo legal. Sobre los datos de titularidad privada, este autor indica que la propiedad de los datos de índole personal depende de la voluntad de su titular y que habrá tantos propietarios cuantos el titular consienta que ostenten tal calidad, recalcando que en todo caso, sólo es propietario el titular; todos los demás dueños de los datos se configuran como copropietarios de los datos de índole personal. Además, agrega este autor que quien conoce el dato o accede a él es poseedor del dato.

---

[491] COHEN, Jessica. op.cit. pág. 1391.
[492] De esta misma idea es Pamela Samuelson quien plantea que la privacidad informacional debe ser protegida por un sistema similar al de la propiedad intelectual. Ver. SAMUELSON, Pamela. op.cit.
[493] RUIZ, Antonio. Los datos de carácter personal: concepto, requisitos de circulación, procedimientos, normativa y formularios. 1999. Barcelona, Bosch. 208p. pág. 43.

Osvaldo Gozaíni[494] reconoce la relación entre derecho de propiedad y protección de datos, al indicar que el derecho a tutelar los datos no se visualiza como un derecho subjetivo, individual y personalísimo. Pareciera plantearse al dato, según este autor, como un problema de propiedad a defender, de manera que las herramientas constitucionales que garantizan la propiedad son aplicables sin mayor dificultad cuando el objetivo es salvaguardar la esfera más personal del individuo[495].

De su parte, Oscar Puccinelli[496] divide el derecho de propiedad sobre la información personal, según se trate del titular de los datos o el titular del banco de datos. Indica respecto del primero, que se trataría de una suerte de derecho de propiedad sobre los datos por parte de las personas a las que se refieren, lo que llevaría, como lógica consecuencia, a sostener que ningún dato podría ser registrado sin el consentimiento de aquellas, y que las limitaciones a este derecho sólo podrían estar fundadas en la ley, y por motivos excepcionales de utilidad común. En relación al segundo, adjudica el derecho de propiedad sobre los datos personales a quien, colectándolos o elaborándolos, los incorpora a su patrimonio, de manera que sólo por motivos excepcionales y en situaciones concretas podría obligarse al propietario a la modificación o exclusión de los datos de los cuales se ha apropiado[497].

Para Noé Riande[498] los datos personales derivan de atributos que se le asignan a la persona de manera que nadie puede tener la presunción de ser propietario de los datos relativos a

---

[494] GOZAINI, Osvaldo. op.cit. pág. 346.

[495] Osvaldo Gozaíni agrega que este raciocinio que señala que la intimidad, la privacidad y la identidad personal son también derechos de propiedad no es nuevo, ya que Warren y Brandeis lo plantearon en su clásica obra sobre la intimidad, ya en 1890, al señalar que "el derecho a ser libre garantiza el ejercicio de un amplio haz de derechos subjetivos; y el término propiedad abarca en su significado actual, todo tipo de derechos de dominio, tanto tangibles como intangibles". GOZAINI, Osvaldo. op.cit pág. 347.

[496] PUCCINELLI, Oscar. 1999. El hábeas data en indoiberoamérica. Santa Fé de Bogotá, Editorial Temis. 607p. pág. 77.

[497] Cita además este autor, una interesante sentencia (T-414 de 1992) de la Corte Constitucional de Colombia, que se refirió a la propiedad sobre los datos luego de indicar que el dato constituye un elemento de la identidad de la persona, por lo que, en criterio del Tribunal, es de su propiedad, en el sentido que tendría ciertos derechos sobre su uso. Ibídem.

[498] RIANDE, Noe. La desprotección de los datos personales. [en línea] <http://infoleg.mecon.gov.ar/basehome/noticias/riandejuarez-30-4.htm> [consulta: 24 noviembre 2003]. Este autor se refiere, asimismo, sobre la naturaleza jurídica del dato, indicando que el dato se trata de un bien mueble, aun siendo intangible, y de uso común ya que sobre el dato no puede hacerse uso de una manera exclusiva como un derecho real, señalando que: "los datos referidos a las personas son bienes de uso común que además de que cualquiera los puede usar, son bienes equiparables a todos aquellos recursos que el Estado administra, determinando las reglas para entregarlos en concesión (aún cuando no se trate de bienes necesariamente destinados a una causa de utilidad pública a cambio de que se genere riqueza y no deterioro, en beneficio del Estado mismo".

su persona, indicando que sobre el dato personal se puede presumir posesión pero nunca propiedad porque, se trata de atributos del individuo sobre los cuales él no puede hacer uso de manera exclusiva como un derecho real. Señalando en forma coincidente con Renato Jijena que si se conserva a los datos almacenados en un soporte magnético puede ostentarse propiedad sobre el recipiente y sobre las diferentes cargas magnéticas que en él se han hecho, pero fuera de ese recipiente los datos personales no son ni de la persona a la cual conciernen ni de quien los conozca.

Otro autor argentino, Leonardo Ghigliani[499] se refiere a la propiedad de los datos personales, a partir de la conceptualización y clasificación del dato, indica que éste es "una representación de una porción de la realidad expresada en términos que forman parte de un código preestablecido de manera que pueda ser interpretado, y que está destinado a dar esa información a un receptor" a partir de esta definición este autor indica los dos elementos del dato, a saber: el código preestablecido que viene a ser las palabras, los números, gráficos, etc. y la realidad que representa, es decir, un objeto, un estado, un acontecimiento, un sentimiento, etc. Luego, razona señalando que el código preestablecido es una expresión comúnmente acordada respecto de la cual difícilmente se pueda asignar propiedad a alguien determinado y que el elemento realidad del dato es el que determina la propiedad del dato y el derecho a su uso. Luego distingue a estos efectos entre la realidad que representa el dato: si esa realidad se refiere a una sobre la cual el sujeto tiene cierto dominio porque se efectúa dentro del ámbito de su intimidad, se puede hablar que este sujeto tiene dominio sobre el dato[500], sin embargo, si el dato representa un hecho natural o un elemento de la realidad que no es susceptible de incorporarse al patrimonio o a la intimidad de algún sujeto, el dato no recae en dominio de nadie y su uso y acceso es libre para todo sujeto. Luego este autor, señala que este dominio sobre el dato da la posibilidad a su titular de otorgar el derecho de uso sobre el dato a un tercero, pero no de transmitir el dominio sobre el dato, ya que los datos siguen la suerte del dominio de la realidad, el cual siempre recae en el titular de esa realidad.

---

[499] GHILIANI, Leonardo. Datos personales: propiedad y derecho al uso. 1998. [en línea] <http://www.it-cenit.org.ar/Publicac/PeopleBases/Recopilac/Recopilac2.htm> [consulta: 24 noviembre 2003]

[500] Aclara el autor a este respecto que utiliza el término dominio no en el sentido jurídico de derecho real de dominio, sino en un sentido de plena facultad exclusiva de uso, acceso, disposición, etc.

En el ámbito nacional algunos autores se han pronunciado sobre la existencia de propiedad sobre información personal, así por ejemplo, Renato Jijjena[501] señala que el derecho de oposición regulado en nuestra ley 19.628 en el artículo 3 inciso final, a propósito de la facultad del titular de datos de oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado y encuestas de opinión, refuerza el principio de que los titulares de los datos personales que les conciernen poseen un derecho de propiedad sobre los mismos, lo que se entiende, según este autor si se tiene presente que se trata de información nominativa o personalísima referida a atributos de su personalidad, en concreto, a la intimidad o privacidad de las personas.

De otra parte, respecto del dato personal y su propiedad debemos distinguir entre el posible titular de ellos, y la etapa del tratamiento en la cual nos encontramos presentes. Es decir, es necesario a estos efectos diferenciar entre una posible propiedad del dato-titular de datos personales y propiedad del dato-titular del banco de datos. Respecto a la segunda relación que efectuamos Renato Jijena[502] opta por negar la existencia de propiedad sobre la información personal que se encuentra almacenada en bases de datos por parte de aquellos que son titulares de dichas bases, ya que son cosas distintas el continente o la estructura de la base o banco de datos que el contenido o la información almacenada en el mismo, y que las normas internacionales sobre propiedad intelectual amparan a las compilaciones de datos cuya selección o disposición de contenidos sean creaciones originales señalando expresamente que dicha protección autoral no abarca la información compilada o a los datos en sí mismos, de manera que los titulares de bancos de datos personales sólo pueden considerarse propietarias intelectuales del diseño y estructura original de fichero computacional, pero no respecto de la información nominativa que se encuentra almacenada en ellos. Una opinión contraria tiene Raúl Bertelsen[503] para quien conforme a las normas constitucionales vigentes resulta indiscutible que la persona que efectúa operaciones de tratamiento de datos y elabora un registro o banco de los mismos, tiene un derecho de propiedad sobre la base de datos que goza de reconocimiento y protección constitucional. Haciendo ver -aun cuando no en forma expresa- que su afirmación se refiere al contenido de la base de datos, es decir, en nuestro caso, a los datos personales, cuando

[501] JIJENA, Renato. 2001. op. cit. pág. 104
[502] JIJENA, Renato. 2001. op. cit. pág. 91.

afirma que el contenido de una base de datos puede, en efecto, representar un activo de gran valor patrimonial y de ahí la importancia de reconocer a su dueño el ejercicio exclusivo de las tradicionales facultades del dominio.

De nuestra parte, creemos que propietarizar la información personal constituye uno de los elementos del modelo de mercado de datos personales que resulta más eficiente, tanto desde un punto de vista puramente económico, como asimismo, desde el enfoque de la finalidad de las normas de protección de datos personales, cuyo objeto esencial es proteger la privacidad informacional de las personas[504].

---

[503] BERTELSEN, Raúl. Datos personales: propiedad privada, libre iniciativa particular y respeto a la vida privada. 2001. En: Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5. pp. 113-129. pág. 121

[504] Este punto será estudiado en profundidad en el Capítulo V de esta tesis, cuando nos refiramos al modelo de mercado de datos personales que proponemos.

CAPITULO V

UN MODELO DE PROPUESTA

5.1. 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[505]. Prueba de ello, son los múltiples proyectos de ley que se han presentado con el objeto de modificar la normativa vigente y que se encuentran actualmente en tramitación en el Congreso Nacional[506].

[505] Estas inconsistencias y vacíos fueron analizados en profundidad en el Capítulo II de esta tesis.
[506] 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 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 N° 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 N° 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 N° 19.628, suspendiendo por un plazo determinado la información comercial de las personas cesantes".
Boletín 4466-03 "Modifica la ley N° 19.628, con el objeto de ampliar los mecanismos de protección de los datos de carácter personal".
Boletín 4482-03 "Modifica la ley N° 19. 628, con el objeto de prohibir la comunicación de información que verse sobre obligaciones que indica, cuando el servicio de ellas se haga a través de descuentos de sus emolumentos por parte de los empleadores".
Boletín 4629-07 Modifica la ley N° 19.628, sobre Protección de la Vida Privada, en materia de rechazo de instrumento de pago.
Boletín 4159-03 "Deroga el decreto supremo N° 950, del Ministerio de Hacienda, de 1928, sobre boletín comercial".
Boletín 4184-03 "Proyecto de ley que modifica la sistematización de información financiera."

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.

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 Nº 19.628, y nos llevan a concluir que en Chile aún está pendiente el tema de la protección de datos personales"[507].

Otro autor nacional, Francisco González[508], plantea la necesidad de reforma de la Ley 19.628, por cuatro razones:

[507] HERRERA, Rodolfo. 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.
[508] GONZALEZ, Francisco. op.cit. pág. 177.

- 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"[509].

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

[509] CERDA, Alberto. op.cit. pág. 97. Otros autores han criticado la normativa vigente en Chile con similares argumentos. V. a. JIJENA, Renato. "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, C. "Breve análisis de la

sus datos a terceros distintos del responsable del registro (mercado secundario), lo que aumenta la asimetría de información; 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.

5.2. Algunos modelos de protección de datos personales.

A continuación revisaremos cuatro 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.

---

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].

5.2.1.- Modelo tradicional de protección

Julie Cohen[510] que tiene una mirada conservadora y más 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:

- Debe encontrar un equilibrio entre la propiedad y la libertad de expresión.[511]

- 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 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.

- 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

[510] COHEN, Julie. op. cit. pág. 1428.
[511] 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.

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[512] 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.

5.2.2.- Modelo de propietarización en base a una inalienabilidad híbrida

Paul Schwartz[513] 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.* 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.

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.

- 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[514] y responder a la necesidad de obtener privacidad informacional[515]. Estas

[512] COHEN, Julie. op. cit. pág. 1430.
[513] SCHWARTZ, Paul. op. cit. pág. 2060.
[514] Señala Paul Schwrtz 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 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, Paul. op. cit. pág. 2097.
[515] 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

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"[516], 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.

- Normas legales supletorias: Paul Schwartz establece el uso de *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. Este *default* 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*.

- 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.

- 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

---

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 P. op. cit. pág. 2098.

[516] SCHWARTZ, Paul. op. cit. pág. 2098.

suficientemente altos que evitan potenciales violaciones y fomenta la interposición de acciones que tengan por objeto defender las asignaciones en materia de privacidad.

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

5.2.3. Modelo basado en la distinta naturaleza de los datos personales

Stan Karas[517] 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[518] 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 debe 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 es 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.

[517] KARAS, Stan. op. cit. pr. 110.
[518] Stan Karas entiende por identidad cualquier información que pueda distinguir a un individuo.

5.2.4. 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, 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 produce 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 creditito u otra información financiera[519].

5.2.5. Modelo mercado nacional de información

Keneth Laudon[520] 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:

[519] PRIVACY RIGHT. Control of personal infromation. The economic benfits 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]
[520] LAUDON, Keneth. op.cit. pág. 1.

a) 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.

b) El modelo debe distinguir entre los distintos tipos de datos personales que son tratados en el mercado, de manera que sea eficiente.

c) Se deben establecer reglas de responsabilidad que desincentiven al que efectúa tratamiento de datos a infringir la normativa aplicable.

d) El control del titular de los datos debe estar presente también en el mercado secundario de datos personales.

5.3. Propuesta concreta de modificación al modelo regulatorio chileno en materia de protección de datos personales.

Como se ha podido observar del Capítulo II de esta tesis -que trata en profundidad la normativa chilena en materia de protección de datos personales- 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 v/s 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[521]; 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[522], entre otros. Lo

[521] 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, 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".

[522] 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

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. De otra parte, como se observara en el capítulo anterior, 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, donde 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 en una o múltiples ocasiones que es personal sin tener que pagar ninguna compensación[523]. 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, es necesario plantear, 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

---

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 inversionista 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, la multa a aplicar conforme estas normas es la chilena, 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. Asesor Jurídico de la División Tecnologías de la Información de la Subsecretaría de Economía, Fomento y Reconstrucción.

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 son 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 cerificar 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 v/s 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

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

mejor desde un punto de vista de eficiencia económica, en vez de imponer una solución legal que les obligue a revelar o mantener oculta los 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 no sólo las críticas y deficiencias observadas por esta tesista, sino que también aquellas efectuadas por la doctrina nacional. Este modelo, que 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 protección; iv) Control del titular de los datos personales; v) Responsabilidad y régimen sancionatorio, los que pasaremos a revisar a continuación.

5.3.1. 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[524] 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[525]. 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

[524] CAVOUKIAN, Anne. 1999. op.cit. pág. 18.
[525] Ibídem.

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 éste 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.

5.3.2. 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 adquirente 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[526].

[526] VARIAN, Hal. 1996. Economic aspects of personal privacy. [en línea] <http://www.sims.berkeley.edu/~hal/Papers/privacy/> [consulta: 02 febrero 2005].

Debemos tener presente en nuestro modelo el tema de 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, dado 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.

Concluyendo, para que las transacciones sobre los datos personales (contratos) puedan ocurrir eficientemente, hay varios requisitos previos: Costos de transacción suficientemente bajos[527]; 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.

5.3.3. 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[528], dependiendo cuál de estas dos variables sea más fácil medir en un momento determinado. Creemos que en ambos casos, es el 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 v/s el costo en que incurren los que desean acceder a los datos personales, debido a que existen mayores trabas 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 sí 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 v/s 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[529].

Compartimos con Lawrence Lessig[530], 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

---

[527] 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.

[528] 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. COOTER, R. y ULEN, T. op.cit. pág. 129.

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

> - 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).
> - 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 a otra. Así la propiedad protege la posibilidad de elegir, la responsabilidad protege la transferencia.
> - 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.

---

[529] Para una mejor comprensión de estas reglas ver el Anexo de esta tesis.
[530] LESSIG, Lawrence. 2001. op.cit. pág. 295.

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 los datos, 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[531].

[531] SCHWARTZ, Paul. op. cit. pág. 2074.

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[532]en el esquema siguiente:

a. 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".

b. 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.

c. 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).

d. 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".

5.3.3.1. 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

[532] Teniendo presente que, como señalan Melamed y Calabresi, la mayoría de los derechos son mixtos. Ver Anexo de esta tesis.

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 efectuó 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 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 personas jurídicas privadas.

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 protegida 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 protegida por reglas de propiedad.

g) Datos penales.

Derecho a la privacidad informacional protegida por reglas de responsabilidad.

h) Datos públicos.

Derecho a la privacidad informacional protegida por reglas de responsabilidad.

i) Datos en general

Derecho a la privacidad informacional protegida 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.

5.3.3.2. 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.

5.3.3.2.1. 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 de 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.

5.3.3.2.2. 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, aún 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 accesible 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 registro 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 aun 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 maluso) 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.

5.3.4. 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.

5.3.4.1. 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[533].

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[534]. 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

[533] 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].
[534] Ibídem.

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 requiere 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, 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 que existan consentimientos o autorizaciones generales para efectuar tratamiento de datos personales, siempre que se cumplan con todos los requisitos expuestos anteriormente.

5.3.4.2. 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 aún 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.

5.3.5. 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.

5.3.6. 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.

5.4. 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 esta tesis, 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 un gradual disminución en el nivel de protección disponible al público en general"[535]

De su parte, Eli Noam[536] 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

[535] 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].
[536] NOAM, Eli. op.cit. pág. 12.

universalmente a pesar de la riqueza, pero está en la naturaleza del humano poseer preferencias y necesidades que varían, y cambiar lo que ellos tienen por lo que ellos quieren. 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, y por lo tanto, 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"[537].

Por otra parte, Daniel Solove[538] 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, sumiendo 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, y entonces la determinación del valor de la información es incierta"[539]. 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 esta tesis 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

[537] FROOMGIN, Michael. op.cit. pág. 1535.
[538] SOLOVE, Daniel. 2004. The digital person. Technology and privacy in the information age. New York, New York University Press. 283p. pág. 81.
[539] SOLOVE, Daniel. op.cit. 87.

primera transacción.

Julie Cohen[540] establece dos opciones respecto de los costos que genera la protección de la privacidad informacional. Indica que establecer los costos de cargo de los que efectúan tratamiento de datos y de los usuarios de la información personal, promoverá mayor respeto por la dignidad de los individuos que exigir a éstos que compren su privacidad apoyado en una regla legal de "no-privacidad". Señala esta autora, que bajo la primera asignación de costos, los costos de la privacidad son asumidos por la sociedad en general; bajo la otra, los costos son asumidos por aquellos individuos que desean privacidad y pueden permitirse pagar por ella.

[540] COHEN, Julie. op. cit. pág. 1390.

Conclusiones

Como habrá podido concluir el lector de la presente tesis, 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.

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.

En este escenario, se planteó como hipótesis que este mercado era uno en el cual existían ciertas fallas, y que además se encontraba regulado por una normativa que no asignaba eficientemente las titularidades, y que asimismo era una norma que establecía derechos confusos y poco delimitados, considerando que no se encontraban en ella regulados ciertos temas que resultan esenciales para toda ley que reglamente este ámbito.

Durante la investigación efectuada, se comprobó que la hipótesis expuesta era la correcta, ya que del estudio pormenorizado de la norma pudimos comprobar que en ella existía una asignación de titularidades que resultaba ineficiente desde un punto de vista económico, debido a que los agentes de este mercado podrían encontrarse en una situación mejorada, desde el punto de vista de la eficiencia de Kaldor-Hicks, ya que empleando una nueva regulación los que ganan más (titulares de bancos de datos) pueden compensar a los que ganan menos (titulares de datos). Por otra parte, existe una mayor eficiencia en este nuevo estado regulatorio, en el cual existe una producción óptima de información personal, en vez de un estado en el cual existe una sobreproducción de dicha información, que es generada por la no internalización por parte de los titulares de los bancos de datos de las externalidades negativas que afectan a los titulares de los datos personales.

Este nuevo estado regulatorio se basa en el modelo de autonomía que se expuso en el Capítulo V de esta tesis. El 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 sus 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 la diversidad de los datos personales.

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, como se pudo observar en el Capítulo IV y V de la presente tesis, 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.

Esperamos que la presente tesis entregue a nivel nacional, un aporte innovador a las críticas efectuadas al régimen regulatorio aplicable al tratamiento de datos personales en Chile, desde que el enfoque aquí utilizado es económico y por lo tanto enfocado al bienestar social de la economía chilena, logrando asimismo, proteger con mayor fuerza la privacidad informacional de los individuos.

ANEXO

GENERALIDADES DEL ANÁLISIS ECONÓMICO DEL DERECHO Y DE LA TEORÍA ECONÓMICA DE LA PROPIEDAD

1. El análisis económico del derecho.

1.1. Concepto

La economía[541] estudia la manera en que las sociedades utilizan los recursos escasos para producir mercancías valiosas y distribuirlas entre los diferentes individuos[542]. Su objeto de estudio de puede ser enfocado desde dos puntos de vista: el primero, que busca estudiar las economías explicando su funcionamiento tal cual es en la realidad (enfoque positivo), y el segundo, que elabora prescripciones basadas en la economía positiva y en juicios de valor, ocupándose, por lo tanto, del "deber ser" de la actividad económica (enfoque normativo)[543]. A su vez, la economía se divide en dos grandes áreas, la microeconomía que estudia la manera en que eligen los individuos en condiciones de escasez, observando las decisiones de los individuos y el comportamiento colectivo en cada mercado[544], y la macroeconomía, que se centra en conjuntos más amplios de mercados, así, por ejemplo, trata de explicar la tasa de desempleo, el nivel global de precios y el valor total de la producción nacional[545].

Desde un punto de vista histórico, el derecho y la economía se han visto entrelazados desde antiguo, así como señala Carlos Floriano, ambas ciencias tienen un mismo objeto de estudio, el contexto social, y, al mismo tiempo, condicionan una misma realidad. Así, los

---

[541] El Diccionario de la Real Academia de la Lengua Española, define a la economía como la ciencia que estudia los métodos más eficaces para satisfacer las necesidades humanas materiales, mediante el empleo de bienes escasos. DICCIONARIO DE LA LENGUA ESPAÑOLA. Vigésima segunda edición [en línea] < http://www.rae.es/> [consulta: 18 marzo 2005].
[542] SAMUELSON, Paul y NORDHAUS, William. 2002. Economía. 17a ed. Madrid, McGraw-Hill. 387p.
[543] COLOMA, Germán. Apuntes para el Análisis Económico del Derecho Privado Argentino. 1999. CEMA Working Papers Universidad del CEMA. 156p.
[544] El AED se basa en los principios microeconómicos.
[545] FRANK, Robert. Microeconomía y conducta. 2001. 4ª ed. Madrid, Mc Graw-Hill. 595p. A su vez, como señala Paul Samuelson, "la microeconomía es la rama de la economía que se ocupa actualmente de la conducta de las entidades individuales como los mercados, las empresas y las economías

economistas cuando tratan de explicar la sociedad chocan con las normas jurídicas que influyen, neutralizando o dinamizando, el acontecer económico. Igualmente, los juristas cuando miran el contexto social que trata de ordenar la norma, se encuentran con los hechos económicos como algo insoslayable[546].

Sin embargo, esta interacción entre la economía y el derecho era más bien limitada hasta hace poco tiempo; el derecho confinaba el uso de la economía a las áreas de las leyes antimonopólicas, las industrias reguladas, los impuestos y la determinación de daños monetarios[547]. Esta situación de interacción restringida, cambió desde la década del sesenta, cuando la utilización de la economía se expandió al sistema legal en su mayor amplitud, analizando áreas como los daños, los contratos, la restitución y la propiedad; la teoría de la legislación y la regulación; a la imposición de la ley y la administración judicial; e incluso al derecho constitucional, el derecho primitivo, el derecho naviero, el derecho familiar y la jurisprudencia[548].

Este nuevo campo de interacción entre ambas ciencias, es conocido como análisis económico del derecho[549], en adelante AED, cuyo objetivo esencial es analizar y evaluar el papel de las normas jurídicas dentro del funcionamiento de los mercados, a través del estudio de su impacto sobre el comportamiento de los agentes económicos y su repercusión en las cantidades y los precios[550]. También se le ha definido como la aplicación de la teoría económica y de los métodos econométricos para examinar la formación, estructura, procesos e influencia de la ley y

---

domésticas y la macroeconomía, es la rama de la economía que se ocupa del funcionamiento global de la economía". SAMUELSON, Paul y NORDHAUS, William. op. cit. pág. 5.

[546] FLORIANO, Carlos. Derecho y economía. Una aproximación al análisis económico del derecho. 1998. Badajoz, Universidad de Extremadura. Servicio de publicaciones. 190p.

[547] COOTER, Robert y ULEN, Thomas. op.cit. En el mismo sentido, COLOMA, Germán. op. cit. pág. 2. quien señala que el análisis de las normas jurídicas tiene una tradición relativamente larga en lo que se refiere a disposiciones relacionadas con impuestos y otras actividades directamente encaradas por el estado, tales como políticas de gasto social y regulación de servicios públicos. Esta parte de la disciplina forma el área de las finanzas públicas o de la economía del sector público.

[548] POSNER, Richard. 1998. El análisis económico del derecho. México D.F. Fondo de Cultura Económica. 682p.

[549] También se le denomina "Derecho y economía" por la traducción de "*Law & economics*". Se suele reconocer como precursores de este movimiento a Guido Calabresi con su estudio sobre los daños y a Ronald Coase sobre el costo social, ya que fueron los primeros intentos por aplicar sistemáticamente el análisis económico a áreas del derecho que no regulan expresamente relaciones económicas. POSNER, Richard. op. cit. pág. 27 y ROEMER, Andrés. Introducción al análisis económico del derecho. 1994. México D.F. Fondo de Cultura Económica. 114p.

[550] COLOMA, Germán. op. cit. pág. 2.

de las instituciones públicas[551]. Tal como la economía, el AED presenta dos facetas, una positiva y otra normativa, Germán Coloma[552] señala que el análisis positivo busca explicar el efecto de las normas jurídicas sobre los distintos mercados y en ciertas circunstancias produce además teorías que pretenden encontrar causas económicas en la adopción de ciertas normas por parte de las distintas sociedades. El análisis normativo, en cambio, sirve para brindar prescripciones respecto de cuáles normas jurídicas son más adecuadas en una situación o en otra, según cuál sea el objetivo buscado por el legislador. En términos más simples, Andrés Roemer señala que la diferencia entre el AED positivo y normativo, es que el primero busca explicar el mundo tal cual es, y el segundo, trata de cambiarlo, para hacerlo mejor[553].

1.2. Metodología utilizada por el AED

En este acápite seguimos a Edmund W. Kitch[554], quien señala como los principales métodos analíticos asociados con la perspectiva tradicional del análisis económico del derecho, los siguientes[555]:

a) Se concibe el objeto de estudio (en nuestro caso, la ley) como un sistema de restricciones y recompensas que interactúa con los individuos. De manera, que se busca analizar la interacción de las normas y los individuos, con el objeto de definir los efectos de dichas normas. Las normas legales conllevan precios implícitos que pueden incentivar o desincentivar a los sujetos a comportarse de un determinado modo.

b) Se busca identificar el componente sistemático de los fenómenos y separar ese componente de los fenómenos aleatorios. Esto es, efectuar conclusiones generales, a partir de los rasgos o características comunes de los objetos de estudio.

---

[551] ROEMER, Andrés. 1994. op.cit. pág. 6., citando a CHARLES K. R., 1989 "Public choice and the economic analysis of law". EN Nicholas Mercuro (org.), Law and Economics, Boston, Kluwer Academic Publishers. 123-173p.
[552] Ibídem.
[553] ROEMER, Andrés. op. cit. pág. 12.
[554] KITCH, Edmund. 1983. The intellectual foundations of law and economics. En: Journal of legal education, vol.33, N° 2. pág. 183-209. Citado por ROEMER, Andrés, op.cit. pág. 16.
[555] ROEMER, Andrés. op. cit. pág. 15.

c) Los actores privados se motivan exclusivamente por el deseo de maximizar su propio interés económico. La referida premisa permite predecir si los individuos cambiarán su comportamiento para evitar los costos de las leyes y obtener sus beneficios.

d) La necesidad de examinar tanto los efectos marginales como totales, con especial énfasis en los primeros, debido a que es importante para entender la respuesta humana a la ley.

e) Los bienes y servicios son multidimensionales, y la regulación de una dimensión afectará las otras dimensiones del bien o servicio.

f) Al evaluar los efectos de la ley, es importante la respuesta transaccional privada de varios individuos. De manera, que deben observarse, más allá de las reacciones de un particular a una norma legal, las respuestas sistemáticas abiertas de un grupo de personas.

g) Al evaluar arreglos regulatorios al mercado, es importante comparar el arreglo que se está evaluando con otras alternativas institucionales viables.

h) Los informes jurídicos y los expedientes de casos (jurisprudencia) contienen información útil acerca de las prácticas económicas particulares.

i) El estudio de la historia de la ley y del derecho comparado es importante, en el análisis económico que se efectúe de cualquier instituto legal.

1.3. Críticas al AED[556].

Es posible agrupar en cuatro las críticas que se efectúan al AED, las referidas críticas suelen ser contestadas, a su vez, por los partidarios de este tipo de enfoque, en base a criterios económicos.

Una primera crítica que se efectúa al AED, es que los fundamentos normativos del enfoque económico son tan repulsivos que resulta inconcebible que el sistema legal los adopte. Richard Posner, contesta esta crítica señalando que "no debemos rechazar todo el análisis económico del derecho sólo porque no nos convenza la versión más agresiva de tal análisis. La versión más agresiva sostiene que la economía no sólo explica las reglas e instituciones del sistema legal, sino que provee la guía más sensata desde el punto de vista ético para el mejoramiento del sistema. Podríamos creer que la economía explica sólo unas cuantas reglas e instituciones legales, pero que puede utilizarse para mejorar muchas de ellas; o que explica muchas de ellas…"[557].

Se señala como segunda crítica a este enfoque, que no ha podido explicar todas las reglas, doctrinas, instituciones y resultados importantes del sistema legal, a la que Richard Posner responde indicando que "…un hincapié exagerado en los acertijos, las anomalías y las contradicciones no se justifica cuando se habla de un campo de la investigación tan reciente y sin embargo tan fructífero, y también se olvida así una lección importante del progreso científico: a menos que esté totalmente errada, una teoría no se destruye señalando sus defectos o limitaciones, sino proporcionando otra teoría más incluyente, más poderosa, sobre todo más útil" [558].

Se critica además que el AED tiene un sesgo ideológico conservador y liberal, frente a posiciones más socializantes, o en otras palabras, se apoyan como mejores soluciones las que da el mercado, en lugar de las que se derivan de la intervención estatal. Floriano Corrales señala a

[556] Este acápite contiene fundamentalmente las ideas expuestas sobre la materia por Richard Posner, POSNER, Richard. op. cit. pág. 30 y Carlos Floriano, FLORIANO, Carlos. op cit. pág. 29.
[557] POSNER, Richard. op. cit. pág. 31.
[558] Ibídem.

este respecto que "debemos preguntarnos si el análisis que se hace es bueno o malo y si los resultados de los mismos ayudan o no a diseñar una adecuada política jurídica, más que a determinar el carácter ideológico de los mismos"[559]. De su parte, Richard Posner señala que "la crítica también omite varios hallazgos de los analistas económicos del derecho…referentes al derecho de tener un defensor y de presentar pruebas en los juicios penales, a la fianza, la responsabilidad objetiva… los costos sociales del monopolio, los daños en los casos de injurias personales, la regulación del sexo y muchos otros que apoyan a las posiciones liberales"[560].

Por último, se suele criticar al AED porque olvida a la justicia. Frente a esta aseveración, Richard Posner señala que se debe distinguir entre los diferentes significados de justicia, señalando que a veces significa justicia distributiva, es decir, el grado adecuado de igualdad económica, indicando que los economistas tienen mucho que decir acerca de las magnitudes reales de la desigualdad en diferentes sociedades y períodos, acerca de la diferencia entre la desigualdad económica real y las desigualdades del ingreso pecuniario, etc. y que a veces significa eficiencia; cuando los individuos califican de injusto el hecho de condenar a una persona sin someterla a juicio, de expropiar sin una compensación justa o de no obligar a un automovilista a que pague los daños causados a la víctima de su negligencia, esto no significa nada más que la afirmación de que ese comportamiento desperdicia recursos. No obstante lo anterior, reconoce que la justicia es algo más que la eficiencia, algo más que la economía, pero que sin embargo, "la economía podrá siempre proveer una aclaración del valor mostrando a la sociedad lo que debe sacrificar por alcanzar un ideal no económico de la justicia…"[561].

2. Algunos conceptos elementales

Debemos revisar algunas nociones básicas de economía a objeto de poder adentrarnos con cierto conocimiento en la revisión de la teoría económica de la propiedad; dichas nociones se relacionan con conceptos económicos específicos y de amplia utilización cuando se habla de AED, a saber: eficiencia, maximización, mercado y equilibrio.

[559] FLORIANO, Carlos. op cit. pág. 31.
[560] POSNER, Richard. op. cit. pág. 32.
[561] Ibídem.

2.1. Eficiencia.

Los economistas han entendido la eficiencia de distintas maneras, estableciendo a lo menos cuatro nociones de ella[562], a saber: la optimalidad de Pareto, la superioridad de Pareto, la eficiencia de Kaldor-Hicks y la maximización de la riqueza de Posner[563]. Analizaremos brevemente cada una de ellas.

a) La optimalidad y superioridad de Pareto: Estas nociones implican la clasificación de un estado de cosas. Un estado de cosas, X, es superior en términos de Pareto a otro estado, Y, sí y sólo si el moverse de X a Y no deja a ningún individuo peor que antes y hace que al menos un individuo mejore. Un estado de cosas es óptimo en términos de Pareto, si ningún estado de cosas es superior a él en términos de Pareto; es decir, si cualquier alejamiento con respecto a ese estado de cosas hace que por lo menos un individuo empeore[564]. En otras palabras, una situación es óptima en términos de Pareto, si es imposible mejorar el bienestar de un individuo sin empeorar el de alguna otra[565]. En la práctica, sin embargo, la mayor parte de las políticas producen ganadores y perdedores, de manera que la eficiencia paretiana no alcanza a evaluar estas situaciones. Para hacer frente a este problema, Kaldor-Hicks-Scitovsky desarrollaron la idea de compensación potencial.

b) Eficiencia de Kaldor-Hicks: La eficiencia según Kaldor-Hicks o mejora potencial en términos de Pareto, indica que un estado de cosas, X, es eficiente en términos de Kaldor-Hicks a otro estado, Y, si después de moverse de X a Y los ganadores pueden compensar

[562] COLEMAN, Jules. Efficiency, utility and wealth maximization. 1980. EN: Hofstra Law Review, vol.8, Nº 3. pág. 512. Citado por ROEMER, Andrés. op.cit. pág. 26.
[563] Existe, asimismo, otro tipo de eficiencia, que no dice relación con las preferencias individuales sino que con la producción, respecto a esta eficiencia en la producción o productiva, se han entregado diversas definiciones, así, para Roemer la eficiencia productiva que significa que todos los factores de la producción se han asignado en un espacio productivo, de tal modo que ninguna asignación ulterior aumente el producto final. ROEMER, A. op.cit. pág. 26. O bien, puede decirse que un sistema de producción es eficiente si para alcanzar un determinado nivel de producción, dada una situación de la tecnología, no se puede encontrar otro que use menos factores productivos para alcanzarlo, es decir, que la empresa elija el nivel de producción usando el menor número de factores posibles. FLORIANO, C. op cit. pág. 38. Asimismo, se indica que estamos en presencia de eficiencia productiva (aplicando la eficiencia de Pareto) cuando una asignación de recursos es eficiente en la producción o técnicamente eficiente si ninguna reasignación más permitiera producir una cantidad mayor de un bien sin reducir necesariamente la producción de ningún otro. NICHOLSON, Walter. Teoría microeconómica: principios básicos y aplicaciones. 1997. Madrid, McGraw-Hill, 1997. 599p.
[564] ROEMER, Andrés. op.cit. pág. 27.
[565] FRANK, Robert. op.cit. pág. 494.

a los perdedores. Así, como lo señala Andrés Roemer[566], en comparación con el criterio de Pareto que exige moverse de un estado social a otro que no produzca perdedores, la satisfacción del criterio de Kaldor-Hicks requiere que los ganadores den alguna compensación a los perdedores. Puesto que la eficiencia en términos de Kaldor-Hicks nos permite comparar los estados de cosas que involucran tanto a perdedores como a ganadores, dicha noción de eficiencia amplía la clasificación de Pareto.

La mejora potencial en términos de Pareto permite los cambios donde hay ganadores y perdedores, pero exige que los ganadores ganen más de lo que pierden los perdedores. Si se satisface esa condición, los ganadores pueden, en principio, compensar a los perdedores y quedarse todavía con un excedente. Es muy importante recalcar que para una mejora potencial en términos de Pareto, no tiene que hacerse efectivamente la compensación, pero ella debe ser posible en principio[567].

La siguiente tabla explica las diferencias entre la eficiencia de Pareto y la de Kaldor-Hicks[568], bajo los supuestos que existen dos individuos, X e Y, y que el nivel de utilidad que alcanzan, según su percepción, es el que se refleja en la tabla en la situación I. Posteriormente se realiza una nueva asignación de los bienes, de tal forma que la valoración que realizan los individuos es la que se refleja en la situación II. Se observa que la situación II respecto a la I es una situación eficiente desde el punto de vista paretiano, pues ambos individuos mejoran, se ha encontrado una nueva asignación de bienes en que todo el mundo gana. No sucede así en la situación III respecto a la II, puesto que aunque X gana, Y pierde. Sin embargo, esta situación sí sería eficiente desde el punto de vista de Kaldor-Hicks pues lo que gana X es más de lo que pierde Y. La asignación de IV es sólo eficiente desde el punto de vista de Kaldor-Hicks respecto a la III y la V no es eficiente respecto a la IV desde ningún punto de vista.

Tabla Nº 3

[566] Ibídem.
[567] COOTER, Robert y ULEN, Thomas. op. cit. pág. 66.

	I	II	III	IV	V
X	1.000	1.500	1.800	1.700	1.200
Y	100	150	125	500	100
X + Y	1.100	1.650	1.925	2.200	1.300

c) Eficiencia según Posner: Andrés Roemer visualiza todavía otro criterio de eficiencia esbozado por Richard Posner, como una manera de evitar el utilitarismo y los criterios de Pareto como modelos de eficiencia[569]. Este criterio es denominado por el propio Posner como "de maximización de la riqueza/Kaldor-Hicks"; lo que postula Posner es reemplazar la utilidad por riqueza, ya que medir la riqueza en una unidad monetaria resulta mucho más sencillo que medir la utilidad que resultará siempre subjetivo, así "el problema de comparabilidad interpersonal no se presenta porque los dólares, al contrario que las utilidades, son comparables interpersonalmente"[570]. Aplicando el principio anterior a Kaldor-Hicks, se indica que un cambio eficiente en los términos de Kaldor-Hicks que implique un incremento de la riqueza más que en las utilidades sería maximizador de beneficios[571].

El propio Posner dice que el principio de la maximización de la riqueza entraña, primero, una asignación inicial de derechos individuales (a la vida, a la libertad y al trabajo) a sus titulares naturales; segundo, mercados libres que permitan reasignar periódicamente esos derechos a otros usos; tercero, normas legales que simulen las operaciones del mercado en aquellos casos en que el costo de las transacciones de mercado sea prohibitivo; cuarto, un sistema de recursos legales para impedir y corregir la violación de los derechos; y quinto, un sistema de moral personal (las "virtudes protestantes") que sirva para reducir el costo de las transacciones de mercado. Si los campos de acción tradicionales del *Common Law* se reorganizaran de manera más funcional, el primero de ellos sería el correspondiente al derecho de propiedad, el segundo al derecho de los contratos, el tercero al derecho de la responsabilidad extracontractual y el cuarto al derecho procesal y correctivo (incluido el Derecho penal)[572].

---

[568] FLORIANO, Carlos. op cit. pág. 39.
[569] ROEMER, Andrés. op.cit. pág. 32.
[570] ROEMER, Andrés. op.cit. pág. 33.
[571] Ibídem.
[572] POSNER, Richard. Utilitarismo, economía y teoría del derecho. 1998. Revista Estudios Públicos Nº 69:207-257.

De esta manera, Posner plantea que en busca de la asignación eficiente se deberá tener en cuenta el principio de la maximización de la riqueza y que en la referida asignación el incremento en el valor sea bastante grande como para que los ganadores puedan compensar a los perdedores (eficiencia de Kaldor-Hicks).

Por último, resulta interesante mencionar acá los parámetros económicos expuestos por Roemer[573] que se utilizan para abordar la eficiencia de las normas jurídicas. Indica en primer término que todos los beneficios y los costos pueden determinarse en función de un denominador común: el dinero, en todo caso a este respecto subraya que no es esencial para el análisis económico y no excluye aspectos que podrán considerarse como no económicos, como la protección a la vida y la integridad física o psíquica. En segundo lugar, los propios individuos determinan los valores monetarios que hay que asignar a sus beneficios y costos (soberanía del consumidor). Luego, señala que los valores que asignan los individuos a sus beneficios y costos son estables, en el sentido de que no les afectan los cambios en la noción de utilidad pública (preferencias exógenas). Por último, los individuos (y, cuando conviene, las empresas) amplían al máximo sus utilidades/beneficios y reducen sus costos (maximización de utilidades y beneficios).

2.2. Maximización.

El principio que señala que los sujetos son racionales porque buscan obtener el mayor nivel de satisfacción a sus necesidades -sean éstas de cualquier tipo-, es la base de lo que se conoce como maximización. Como señala Cooter y Ulen, "los economistas suponen que todos los actores económicos maximizan algo: los consumidores maximizan su utilidad (es decir, la felicidad o satisfacción), las empresas maximizan sus beneficios, los políticos maximizan los votos, las burocracias maximizan las recaudaciones, las instituciones de caridad maximizan el interés social, etc."[574] Que exista escasez o bienes escasos en la inmensa mayoría de los casos, hace que el individuo deba escoger -ante recursos limitados- entre las diversas posibles

[573] ROEMER, Andrés. op.cit. pág. 22.
[574] COOTER, Robert y ULEN, Thomas. op. cit. pág. 24.

alternativas que se le presentan, la que le parece razonablemente mejor (o que le da mayor satisfacción) dentro de este ámbito de restricciones.

La elección de la mejor alternativa permitida por las restricciones puede describirse matemáticamente como una maximización[575].

La economía se ha centrado en el estudio de la maximización de las empresas y de los consumidores. Se señala respecto de los consumidores que éstos tratan de distribuir su limitado ingreso entre los bienes y servicios disponibles en forma tal que se eleve al máximo su satisfacción, de manera que las personas se ven obligadas a modelar su conducta a la luz de sus limitados recursos económicos. Para la teoría económica de la conducta del consumidor, esto significa que todos los consumidores tienen una suma máxima de dinero que pueden gastar en un lapso dado. El problema del consumidor es el de gastar esta cantidad en la forma que le produzca la máxima satisfacción[576]. Los consumidores así, buscan maximizar su utilidad. El principio se aplica con más o menos los mismos matices respecto de las empresas, el contraste fundamental es que las empresas a diferencia de los consumidores, lo que buscan maximizar no es su satisfacción o felicidad sino que sus beneficios, es decir, la diferencia entre el ingreso total y el costo total, donde este último incluye todos los costos tanto explícitos como implícitos de los recursos utilizados por una empresa, sin embargo, podemos observar que hay una similitud: tanto las empresas como los consumidores jerarquizan sus preferencias y maximizan al elegir la mejor alternativa posible.

2.3. El mercado

El mercado es un mecanismo mediante el cual los compradores y los vendedores pueden determinar los precios e intercambiar bienes y servicios, determinando en forma conjunta su precio y cantidad[577].

Existen distintos tipos de mercados de acuerdo al tiempo y al lugar. Así, todos los compradores y vendedores de una determinada industria se reúnen en un mismo tiempo y lugar

[575] Ibídem.
[576] FERGUSON, C. E. Teoría Microeconómica. 1969. México, Fondo de Cultura Económica. 456p.

para intercambiar bienes y/o servicios por dinero u otra contraprestación de naturaleza pecuniaria, ya sea en un determinado espacio físico o geográfico, dentro del marco de una institución, como por ejemplo son las bolsas de valores, o actualmente en Internet[578].

En un sistema de mercado todo tiene un precio, que es el valor del bien expresado en dinero y que representa los términos en que las personas y las empresas intercambian voluntariamente las diferentes mercancías. Una importante función de los precios es que transmiten señales a los productores y consumidores; los precios coordinan las decisiones de los productores y los consumidores en el mercado. Su subida tiende a reducir las compras de los consumidores y reduce los incentivos para producir, constituyendo de esta manera los precios el engranaje del mercado[579].

2.4. El equilibrio.

El equilibrio, al igual que la eficiencia es un concepto económico transversal, es decir, es utilizado en múltiples aspectos por los economistas en base al equilibrio entre la oferta y la demanda, así podemos hablar de equilibrio en el mercado del trabajo, en el mercado de seguros, de bienes y servicios, etc. De otra parte, está el equilibrio general que se presenta cuando existe igualdad entre el costo marginal social y el beneficio marginal social[580].

El equilibrio desde un punto de vista de la oferta y la demanda, está íntimamente vinculado con la idea de maximización, que recién revisáramos, ya que "el comportamiento maximizador tiende a impulsar a los individuos y grupos hacia un punto de descanso, un equilibrio. En efecto, los actores no buscan un equilibrio: simplemente tratan de maximizar lo que les interesa"[581].

---

[577] SAMUELSON, Paul y NORDHAUS, William. op. cit. pág. 23.
[578] FRANK, Robert. op. cit. pág. 30.
[579] SAMUELSON, Paul y NORDHAUS, William. op. cit. pág. 23.
[580] Este tipo de equilibrio será analizado en el acápite siguiente.
[581] COOTER, Robert. y ULEN, Thomas. op. cit. pág. 25.

En un mercado de competencia perfecta[582], se llama perfectamente competitiva a una industria donde hay tantas empresas que las decisiones individuales de cualquiera de ellas no puede influir sobre el precio de mercado, y donde hay tantos consumidores que las decisiones individuales de maximización de utilidad de cualquier consumidor tampoco pueden afectar el precio de mercado. En tal industria el equilibrio de mercado ocurre en el punto de intersección entre la oferta y la demanda, es decir, cuando la cantidad que los proveedores desean vender es igual a la cantidad que los consumidores desean comprar[583].

2.5. Economía del Bienestar.

La economía del bienestar es una parte de la teoría macroeconómica que explora la forma en que interactúan las decisiones de muchos individuos para afectar el bienestar de un individuo. Acá se plantean las grandes cuestiones de política pública, como por ejemplo, si el estado debe intervenir en el mercado o hasta qué punto los mercados pueden maximizar el bienestar individual[584], es decir, formula y aplica criterios para evaluar propuestas distintas de política pública[585].

Fuertemente vinculado a la economía del bienestar se encuentra el denominado equilibrio general de los mercados que se "alcanza cuando las fuerzas competitivas hayan conducido a la igualdad del beneficio marginal y el costo marginal en el mercado para todos los bienes y servicios"[586], es decir, "cuando el sacrificio de recursos que los consumidores están

[582] Se suelen establecer en los libros de economía, cuatro requisitos para que estemos en presencia de una competencia perfecta: a) Todos los agentes económicos que actúan en el mercado sean tan pequeños, en relación con el total del mismo, que no puedan ejercer una influencia perceptible sobre el precio. b) las empresas deben vender un producto estandarizado, es decir, que los productos que venden las empresas sean homogéneos. d) debe existir libre movilidad de los recursos, de manera que éstos puedan entrar o salir del mercado inmediatamente, en respuesta a atractivos pecuniarios. d) Por último, los consumidores y las empresas deben tener información completa y perfecta. Algunos autores, todavía agregan dos requisitos: que no existan prácticas colusivas. Es decir, no existen acuerdos entre empresas que lleven a modificar el precio y que no se trate de un mercado regulado, la única regla existente debe ser la de la oferta y la demanda.
[583] COOTER, Robert. y ULEN, Thomas. op. cit. pág. 47.
[584] COOTER, Robert. y ULEN, Thomas. op. cit. pág. 60.
[585] FLORIANO, Carlos. op cit. pág. 63.
[586] COOTER, Robert. y ULEN, Thomas. op. cit. pág. 60. Carlos Floriano aclara el concepto, "Los individuos cuando deciden qué cantidad comprar de un bien, igualan la utilidad marginal que les reporta el consumo con el coste marginal del mismo, que es le precio que tienen que pagar; las empresas cuando deciden que cantidad deben producir de un bien igualan el precio que cobran y el costo de producir una unidad adicional bajo estas condiciones, los bienes son asignados eficientemente entre los consumidores, porque es imposible reasignar los mismos sin perjudicar a alguien y, al mismo tiempo, la producción es eficiente, porque no se puedes producir más bienes con los recursos disponibles. Así, cuando en el conjunto social la producción y la distribución de bien se

dispuestos a hacer es exactamente igual al sacrificio de recursos que la sociedad debe hacer para obtener una unidad más de producción"[587]. Este equilibrio general es socialmente óptimo, esto es, es eficiente desde el punto de vista de la producción de bienes y la asignación a los consumidores, ya que las empresas maximizan su beneficio y los consumidores maximizan su utilidad, lo que condiciona el establecimiento inevitable y espontáneo del equilibrio en todos los mercados simultáneamente.

Para lograr este equilibrio general y con él el máximo de bienestar social, es necesario que los mercados sean perfectamente competitivos, es decir, eficientes. Sin embargo, en la práctica es casi imposible encontrar mercados perfectamente competitivos, porque usualmente nos encontraremos con fallas del mercado que impiden las situaciones competitivas, y que justifican que el Estado intervenga. Se suelen señalar por los economistas cuatro fallas del mercado: el monopolio; los bienes públicos, las externalidades y la información asimétrica, a las cuales nos referiremos brevemente a continuación.

a) El monopolio es una estructura de mercado en la que el único vendedor de un producto que no tiene sustitutivos cercanos abastece a todo el mercado. El rasgo clave que distingue al monopolio de la empresa competitiva es la elasticidad-precio de la demanda a la que se enfrenta la empresa, en el último caso la relación elasticidad-precio es infinita; si una empresa eleva el precio aun en forma leve, perderá todas sus ventas, en cambio, en el caso del monopolio, la empresa controla significativamente los precios que puede cobrar[588].

Decíamos que un mercado perfectamente competitivo es aquél en que el costo marginal es igual al beneficio marginal, situación que no se presenta en el monopolio, ya que el beneficio marginal supera al costo marginal, al poder cobrar el monopolista más por los bienes que vende, y por loo tanto, al no operar respecto de él, la elasticidad-precio de la demanda.

Las políticas públicas para corregir los efectos del monopolio consisten en sustituir el monopolio por la competencia dondequiera que ello sea posible a través de las leyes

---

realiza de forma eficiente no se puede encontrar otra situación en la que alguien no sea perjudicado, lo cual es la condición de eficiencia según Pareto". FLORIANO, C. op cit. pág. 64.

[587] FERGUSON, C.E. op. cit. pág. 413.

[588] FRANK, Robert. op. cit. pág. 348.

antimonopólicas, o en regular el precio que cobra el monopolista, en el caso de los denominados monopolios naturales, en donde el estado permite que existan pero regula sus precios como, por ejemplo, en los servicios públicos[589].

Un fenómeno que se encuentra muy cercano al monopolio es el oligopolio, que es "un mercado dominado por unas pocas empresas, cada una de las cuales es consciente de su capacidad para influir en el precio de mercado"[590]. Este mercado se caracteriza por la producción de un bien homogéneo o diferenciado en cuanto a marcas y en la capacidad que tiene cada uno de los productores para influir en las decisiones de sus competidores.

b) Las externalidades son beneficios o costos de una actividad que recaen en personas que no participan directamente de ella[591], cuando se trata de beneficios se habla de externalidad positiva, y de externalidad negativa cuando se trata de costos. Generalmente, los intercambios dentro del mercado son voluntarios o consentidos, de manera que los actores del intercambio captan todos los beneficios y los costos, sin que aquellos que no participen de ese particular intercambio o negociación deban soportar los eventuales costos o favorecerse con los beneficios. Este principio general sufre, sin embargo, excepciones cuando estos beneficios o costos se externalizan, se produce acá una falla de mercado. Un claro ejemplo de externalidad negativa se produce en el caso de la contaminación o, en general, ante cualquier molestia o daño que se produzca a un tercero que no ha participado en la actividad generadora de la molestia o daño. Ejemplifica, de su parte, la externalidad positiva, el caso del sujeto que recoge los frutos que caen del árbol situado en la propiedad de su vecino o, en general, ante cualquier beneficio, satisfacción o utilidad que se produzca a un tercero que no ha participado en la actividad generadora del beneficio, satisfacción o utilidad.

Las externalidades positivas constituyen una falla del mercado debido a que producen que el beneficio marginal social sea mayor que el beneficio marginal privado al no considerarse todos los beneficios que produce una determinada actividad, realizándose esa actividad, consecuentemente, a menores niveles que los que dicta la eficiencia.

[589] COOTER, Robert y ULEN, Thomas, op. cit. pág. 61.
[590] FLORIANO, Carlos. op cit. pág. 62

De su parte, las externalidades negativas como señala Cooter y Ulen[592] implican una falla del mercado porque el generador de la externalidad no tiene que pagar por dañar a otros, de modo que se autocontrola en una medida ineficiente. Tal generador actúa como si los costos que produce fueran nulos (imagine a una empresa contaminadora que asume como nulos los costos de la contaminación que genera), cuando en realidad sí existen costos, pero éstos son asumidos por la sociedad. Desde un punto de vista técnico, el generador de la externalidad produce en demasía, y así crea el daño asociado, porque hay una diferencia entre el costo marginal privado y el costo marginal social, rompiéndose el equilibrio general[593]. Lo anterior, se produce porque el costo marginal del que externaliza es menor que el costo marginal que asume la sociedad, lo que le lleva al existir un costo menor para él, a producir más que lo eficiente. Para recuperar el equilibrio, el generador de la externalidad negativa debe internalizar los costos externos que produce y al hacerlo restringirá su producción al nivel que sea óptimo desde un punto de vista social y no privado.

Las políticas públicas destinadas a eliminar este tipo de falla de mercado, se reducen generalmente al establecimiento de impuestos indirectos en el caso de las externalidades negativas, pues gravando el producto que tiene externalidades negativas a un tipo adecuado, puede eliminarse la pérdida de eficiencia, al incentivar que el productor produzca menos a un nivel eficiente. Respecto a las externalidades positivas, la intervención que efectúa el Estado para evitarlas, son las subvenciones, ya que éstas incentivan a producir en un mayor nivel la actividad que produce los beneficios externos.[594]

c) Los bienes públicos constituyen la tercera falla del mercado. Los bienes públicos se caracterizan por poseer dos propiedades específicas: i) No pueden disminuir, es decir, la utilización de un bien público por una persona no deja menos de ese mismo bien al resto de las personas (también denominado como consumo no rival) y ii) No son excluibles, lo que significa que es imposible o prohibitivo (por el alto costo) impedir que los utilicen las personas que no pagan por usarlos. Así, se le ha definido como mercancías en las que el costo de extender el

---

[591] FRANK, Robert. op. cit. pág. 510.
[592] COOTER, Robert. y ULEN, Thomas. op. cit. pág. 62.
[593] Cooter y Ulen indican que el costo marginal privado es el costo marginal de la producción para el generador de las externalidad, y el costo marginal social es la suma del costo marginal privado y los costos marginales adicionales que se imponen involuntariamente a terceros, por cada unidad de producción. Ibídem.

servicio a una persona adicional es cero y resulta imposible impedir que los disfruten algunos individuos[595].

La literatura económica ofrece muchos ejemplos de bienes públicos, la defensa nacional, construcción de una red de autopistas, la adopción de medidas para mejorar la sanidad pública, la televisión abierta, etc., asimismo entiende que este tipo de bienes constituye una factor de ineficiencia en el mercado, debido a que "no hay razón alguna para suponer que los mercados privados suministrarán la cantidad óptima de bienes públicos puros. De hecho, si es imposible a las personas utilizar el bien, tal vez aparezca imposible que una empresa con ánimo de lucro ofrezca cantidad alguna de este bien"[596].

Dado lo anterior, generalmente son insuficientes los bienes públicos que suministran las empresas privadas, entonces el estado debe intervenir para suministrarlos ya sea en forma directa o subsidiando su existencia en cantidades eficientes. Los costos son asumidos por el Estado, pero neutralizados a través del sistema impositivo.

d) La asimetría de información como cuarta falla del mercado se presenta cada vez que entre dos personas dispuestas a intercambiar, existe un desequilibrio tal de información que impide, en definitiva, el intercambio.

El Estado suele intervenir en estas materias a través de la dictación de leyes que impongan un deber especial de información respecto de aquella parte que la posee, como suele ocurrir por ejemplo en las leyes de protección a los consumidores, en donde se establecen los referidos deberes de información a los proveedores de bienes y servicios.

---

[594] FRANK, Robert. op.cit. pág. 510.
[595] SAMUELSON, Paul y NORDHAUS, William. op. cit. pág. 33.
[596] FRANK, Robert. op.cit. pág. 510.

3. Generalidades de la teoría económica de la propiedad.

3.1 Conceptos preliminares.

Desde un punto de vista legal, se define a la propiedad como una relación jurídica entre un sujeto de derecho y una cosa, que le da sobre ella el señorío más pleno. Nuestro Código Civil indica en su artículo 582 que el dominio que se llama también propiedad, es el derecho real que se tiene sobre una cosa corporal, para gozar y disponer arbitrariamente, no siendo contra ley o el derecho ajeno. Como señala Arturo Alessandri[597], la propiedad es un derecho absoluto, porque otorga al titular de él la plenitud de derechos que un individuo puede tener, es un derecho exclusivo, porque sólo le compete el uso y goce a la persona que es dueña de la cosa y nadie puede oponerse a este uso y goce y es un derecho perpetuo, porque no se extingue con el tiempo. Este derecho de dominio entrega tres facultades a su titular, el derecho de uso, o sea, de servirse de la cosa según sea su naturaleza, de goce, o sea, el derecho de percibir frutos que ella es susceptible de producir y de disponer, es decir, hacer con la cosa lo que a uno le plazca[598].

Este concepto legal de propiedad se aleja del concepto económico de ella, como indica Germán Coloma: "La economía positiva suele tomar a los derechos de propiedad como un dato, que sirve para definir el carácter de oferente o demandante de un agente económico en un mercado. En otras circunstancias, la economía normativa suele analizar la conveniencia de políticas que implican una redistribución o redefinición de los derechos de propiedad entre los agentes económicos, estudiando sus efectos desde el punto de vista de la eficiencia o la equidad"[599]. El AED, de su parte, efectúa una mezcla de ambas perspectivas cuando se refiere a derechos de propiedad, "lo que busca principalmente es explicar (economía positiva) y evaluar (economía normativa) los criterios de asignación de tales derechos a las personas y las limitaciones al ejercicio de los mismos."[600]

---

[597] ALESSANDRI, Arturo. s.a. Derecho Civil. De los bienes. Santiago de Chile, Editorial Lex. Tomo segundo.
[598] Cooter y Ulen definen la propiedad como un conjunto de derechos sobre los recursos que el propietario puede ejercer con libertad y cuyo ejercicio está protegido contra la interferencia de otros. COOTER, Robert y ULEN, Thomas. op. cit. pág. 104.
[599] COLOMA, Germán. op cit. pág. 25.

Ahora bien, a efectos de este acápite entenderemos a la propiedad no desde un punto de vista legal estricto, sino que como una relación que se presenta entre el dueño y los demás sujetos, puesto que la propiedad define qué conductas puede realizar su titular y qué conductas deben soportar los demás en relación a un conjunto de recursos escasos[601]. En relación con este enfoque de la propiedad, la economía da respuestas a cuatro cuestiones esenciales: ¿Cómo se establecen los derechos de propiedad?, ¿qué puede ser objeto de propiedad privada?, ¿qué pueden hacer los dueños con su propiedad? y, ¿qué remedios existen para la violación de los derechos de propiedad?[602] De esta manera, la teoría económica de la propiedad utiliza a la economía para analizar las reglas aplicables a la propiedad, dando respuestas a las preguntas anteriores.

3.2. Teoría de la negociación

Cooter y Ulen indican que la teoría de la negociación constituye el fundamento mismo de la teoría económica de la propiedad[603]. Esta teoría que tiene sus bases en la teoría de juegos, establece ciertos postulados respecto a los intercambios voluntarios entre dos o más agentes. Se parte señalando que hay base para un intercambio voluntario siempre que un agente valúe más un bien que otro agente. Por ejemplo, Pedro valúa su reloj en $1000 y Juan en $2000. Juan quiere tener el reloj de Pedro, y tiene dinero suficiente para comprarlo. Un contrato de compraventa permitirá que el reloj pase de Pedro que lo valúa en $1000 a Juan que lo valúa en $2000, al existir una diferencia de valoración del reloj entre el potencial vendedor y el potencial comprador, existe un margen de negociación, en este caso específico de $1000 ($2000 - $1000), de manera que el intercambio voluntario entre las partes se producirá en cualquier valor entre $1000 y $2000, por ejemplo, $1500. Este intercambio beneficia tanto a Pedro como a Juan; Pedro gana $500 ya que valoraba su reloj en $1000 y Juan también gana $500 ya que valoraba el reloj en $2000. En el caso expuesto, se ha producido un traslado de un recurso (el reloj) desde alguien que lo valoraba menos a alguien que lo valora más, de manera, que se produce un excedente cooperativo, que es el valor creado al trasladar un recurso hacia un uso más valioso (en nuestro ejemplo el excedente asciende a $1000).

---

[600] Ibídem.
[601] FLORIANO, Carlos. op cit. pág. 72.
[602] COOTER, Robert y ULEN, Thomas. op. cit. pág. 103.

El ejemplo anterior muestra una solución cooperativa, en la cual las partes se ponen de acuerdo sobre el precio y logran celebrar el contrato de compraventa del reloj, produciéndose la transferencia de propiedad sobre éste desde Pedro a Juan. Sin embargo, podría haber ocurrido que no se produjera acuerdo entre las partes y no se celebrara, consecuentemente, contrato alguno. En este caso, estamos en presencia de una solución no cooperativa. Ahora bien, incluso en este estado de no cooperación, las partes pueden alcanzar un cierto nivel de bienestar, ya que en nuestro ejemplo, Pedro se quedará con su reloj que valúa en $1000 y Juan se quedará con su dinero, que podrá utilizar en otra cosa distinta. A las ganancias de las partes en una solución no cooperativa se les denomina valores de amenaza, que es de $1000 para Pedro y de $2000 para Juan.

En toda negociación e intercambio voluntario, cada parte debe recibir a lo menos el valor de amenaza o no habrá ninguna ventaja que las incentive a negociar. Cooter y Ulen indican que una solución razonable, es que cada parte reciba su valor de amenaza más una parte igual del excedente cooperativo.

Se concluye, entonces, que todo proceso de negociación consta de tres partes: el establecimiento de los valores de amenaza, la determinación del excedente cooperativo y, el acuerdo sobre los términos para distribuir el excedente de la cooperación.

3.3. Teorema de Coase.

La base del teorema de Coase[604] busca determinar cuál es la asignación de derechos eficiente ante una cierta actividad que interfiere con otra[605]. Cooter y Ulen resumen de buena forma este teorema cuando señalan que “cuando una actividad interfiere con otra, la ley debe

---

[603] COOTER, Robert. y ULEN, Thomas. op. cit. pág. 105. Lo señalado a propósito de la teoría de la negociación se basa fundamentalmente en lo expuesto por estos autores en la obra citada.

[604] Denominado de esta manera por ser planteado por Ronald H. Coase, Premio Nobel de Economía de 1992, en su artículo “The problem of social cost” de 1960, publicado en Journal law and aconomics, Nº 3, págs. 144-171.

[605] Cabe destacar que Coase se basa exclusivamente en criterios de eficiencia para construir su postulado, los criterios distributivos no son tomados en cuenta, no obstante, la asignación inicial de derechos, sí resulta ser esencial desde un punto de vista distributivo, ya que asignar un derecho a una determinada persona en detrimento de otra, la hace más rica en la proporción del derecho asignado que aquella otra persona a la cual no se le asignó el derecho en cuestión.

decidir si una de las partes tiene derecho a interferir o si la otra parte tiene derecho a quedar libre de la interferencia. La eficiencia requiere que se asigne el derecho a la parte que lo valúe más. Cuando las partes respetan la ley en una manera no cooperativa, la asignación legal de los derechos es importante para la eficiencia. Cuando las partes negocian con éxito, la asignación legal de los derechos no importa para la eficiencia. Esto es, si hay una negociación exitosa, el uso de los recursos es eficiente, cualquiera sea la regla legal"[606] Coase indica que si las transacciones de mercado fueran gratuitas, todo lo que importaría (aparte de las cuestiones de equidad) es que los derechos de las distintas partes debieran estar bien definidos y los resultados de las acciones legales fáciles de pronosticar[607]. El tema de la clara y buena definición de los derechos no es menor en el teorema de Coase, de esta manera aun cuando los derechos estén asignados al agente correcto desde un punto de vista de la eficiencia, tal asignación podrá no ser eficiente si no se establece en forma cierta y manifiesta el contenido de los derechos asignados, cuáles son las limitaciones para su goce y qué puede hacerse para remover tales limitaciones.

A lo señalado anteriormente, se debe agregar un nuevo elemento que resulta esencial: los costos de transacción, término que es utilizado por Coase para incluir todos los impedimentos de la negociación[608], como por ejemplo, descubrir con quién deseamos transar, informar a la gente que deseamos intercambiar y en qué términos, conducir negociaciones que lleven a un convenio, redactar el contrato, llevar a cabo la inspección necesaria para asegurarnos de que los términos del contrato se observan[609], de manera que la negociación se efectuará cuando los costos de transacción son nulos. El primer postulado del teorema de Coase se puede resumir así: Cuando las partes pueden negociar sin costos, el resultado es eficiente, cualquiera sea la asignación legal de los derechos de propiedad. Es decir, cuando los costos de transacción son nulos o son bajos en comparación con los beneficios que se obtienen cuando se llega a un acuerdo, las reglas legales no importan para lograr la eficiencia, ya que las partes reasignarán el recurso en aquella que lo valúa más, cosa, que como ya hemos visto es eficiente. Luego, el segundo postulado de Coase, indica que cuando los costos de transacción son significativos, de manera que las partes no pueden llegar a un acuerdo, las normas legales que establecen la asignación inicial de derechos sí son importantes para lograr la eficiencia.

[606] COOTER, Robert y ULEN, Thomas. op. cit. pág. 117.
[607] COASE, Ronald. El problema del costo social. 1992.Revista Estudios Públicos (45): 81-134.
[608] COOTER, Robert y ULEN, Thomas. op. cit. pág. 117.
[609] COASE, Ronald. op.cit. pág. 98.

3.4. Los elementos de los costos de transacción.

Cooter y Ulen[610] distinguen tres tipos de costos de transacción, conforme se va a avanzando en la negociación a la cual están asociados: 1) los costos de la búsqueda, que refieren a aquellos en que se incurre para encontrar a la contraparte en la negociación, estos costos generalmente son elevados cuando se trata de bienes o servicios peculiares y bajos en el caso de aquellos que son estandarizados; 2) los costos del arreglo, esto es, los costos asociados a lograr el acuerdo, como por ejemplo, las conversaciones preliminares, costos de asesoría especializada, la redacción del contrato, etc., este tipo de costo suele ser bajo cuando existe cierto nivel de información simétrico entre las partes respecto del objeto de la negociación y sobre los valores de amenaza y la solución cooperativa, un elemento que aumenta este tipo de costos es la cantidad de partes involucradas, se produce aquí un aumento proporcional del costo a medida que aumentan las partes, y 3) los costos de ejecución, que se van a presentar en aquellas negociaciones que implican acuerdos que se cumplen en el tiempo, pues éstos suelen requerir que se monitoree y fiscalice el cumplimiento del señalado acuerdo, los costos de ejecución serán bajos cuando las violaciones del acuerdo puedan observarse fácilmente y la administración del castigo sea barata.

Según estos autores, los costos de transacción, asimismo, se pueden clasificar en base a su mayor o menor relación con las normas, con el sistema legal, en exógenos y endógenos. Así, los costos recién analizados que son determinados por condiciones más o menos objetivas de la negociación privada entre partes, fuera del dominio de la ley, son denominados costos de transacción exógenos; de su parte, aquellos costos que son determinados por la ley son denominados costos de transacción endógenos, este tipo de costos al ser endógenos al sistema legal pueden ser disminuidos por el propio sistema legal, estimulando la negociación entre privados al reducirse los costos de transacción.

[610] COOTER, Robert y ULEN, Thomas. op. cit.. cit. pág. 121.

3.5. Teoremas normativos de Hobbes y de Coase

El teorema de Coase nos dice que si los costos de transacción no son nulos, una adecuada asignación de derechos de propiedad puede servir para reducir tales costos, estructurando la ley de tal manera que se eliminen o, por lo menos, disminuyan los impedimentos para lograr acuerdos privados. Una forma de lograr lo anterior, es efectuar, como ya se señalara, asignaciones de derechos de propiedad simples y claros, ya que es más fácil negociar cuando los derechos legales son simples y claros, que cuando son complicados e inciertos. Lo señalado anteriormente se resume en el teorema normativo de Coase que indica que "el derecho debe estructurarse de modo que se eliminen los impedimentos para los acuerdos privados"[611].

Al mismo tiempo, el sistema legal debiera propender a minimizar los desacuerdos entre las partes y la falta de cooperación, ya que éstos generan costos. Para minimizar el daño resultante, la ley debería asignar los derechos de propiedad a la parte que los valúe más, ya que de esta manera, la ley vuelve innecesario el intercambio de derechos y se ahorra el costo de una transacción. Este postulado se conoce como teorema de Hobbes y se puede resumir en que se debe estructurar la ley de manera tal que se minimice el daño producido por las fallas de los acuerdos privados[612]. Como señala Germán Coloma, "si resulta posible aplicar este principio, los costos de transacción resultan menos importantes como un impedimento para llegar a una asignación eficiente de los recursos económicos, ya que dicha asignación pasa a depender menos de las transacciones (que se vuelven menos necesarias)."[613]

Finalmente, la mala asignación de un derecho efectuada por la ley, que ocurrirá cuando ésta asigna el derecho a quien lo valúa menos, puede ser corregida mediante el intercambio

[611] COLOMA, Germán. op. cit. pág. 33. Germán Coloma, da un buen ejemplo de la aplicación del teorema normativo de Coase aplicado a un caso práctico: Si, por ejemplo, no resulta claro si una persona tiene derecho a utilizar la pared medianera que separa su inmueble del de su vecino para realizar determinada obra, la ejecución de la misma implicará primero la necesidad de que ambos vecinos definan quién tiene derecho a hacer qué cosa en dicha pared medianera. Si las reglas de aprovechamiento de las medianeras están en cambio bien definidas (es decir, si los derechos de propiedad sobre las mismas están bien separados entre los vecinos), la construcción de la obra en cuestión implicará simplemente el ejercicio de un derecho originario o a lo sumo una negociación para determinar un pago compensatorio de un vecino al otro. Ibídem.
[612] COOTER, Robert y ULEN, Thomas. op. cit. cit. pág. 129.

privado del derecho entre las partes, pues tal intercambio generará un excedente positivo para las partes. La eficiencia, en todo caso, exige que tal intercambio se produzca sólo en el caso en que el excedente producto del intercambio sea mayor que los costos de transacción de la respectiva negociación, pues de lo contrario, el intercambio no se producirá.

4. Especial referencia al estudio de Melamed y Calabresi[614]

Cuando hablamos de la posibilidad de acceder y conocer la información personal de otro, estamos en presencia de un conflicto de intereses, de un choque entre distintos bienes jurídicos: la privacidad v/s derecho a la información. En este escenario, el Estado debe decidir a cuál de las partes favorecer, en nuestro caso, si favorecer a la persona a la cual se refiere la información, también denominada titular de datos personales, o si favorecer a la persona que desea acceder a esa información[615]. Según Calabresi y Melamed, este es el primer asunto que cualquier sistema jurídico debe encarar ante un conflicto de intereses entre dos personas, el problema de la "titularidad de los derechos", en él el rol del Estado es decidir cuál de las partes en conflicto tendrá el derecho a prevalecer.

4.1. Asignación de las titularidades

Pero, ¿a qué parámetros atender en la asignación de titularidades en un caso determinado? Se entregan por estos autores tres criterios para esta asignación de titularidades: la eficiencia económica, preferencias distributivas y otras razones de justicia.

Así, según Calabresi y Relamed, la eficiencia económica indica que se deberá asignar aquella titularidad que implique una asignación de recursos eficiente en el sentido de Kaldor-Hicks, cuando indican que "la eficiencia económica requiere que elijamos el conjunto de derechos que conduciría a aquella asignación de recursos que no podría ser mejor, en el sentido

---

[613] COLOMA, Germán. op. cit. pág. 33

[614] En este apartado efectuaremos una revisión de los aspectos más relevantes que expusieron los profesores Guido Calabresi y Douglas Relamed, en su conocido artículo "Property rules, liability rules, and inalienability: one view of the catedral" publicado en Harvard Law review, Vol. 85, Nº 6 (1972), pp.1089-1128.

[615] Existen innumerables ejemplos de este tipo de conflictos, v.gr. el derecho a contaminar versus el derecho a vivir en un medio ambiente libre de contaminación; el derecho de los autores sobre sus

de que un nuevo cambio no mejoraría tanto la condición de aquellos que ganaron con él como para que éstos compensaran a aquellos que perdieron e, incluso así, quedaran mejor que antes del cambio". En un mundo en donde los costos de transacción son una realidad, estos autores entregan determinadas pautas en orden a efectuar una asignación de titularidades eficiente, las cuales son presentadas en orden de prelación, de manera que ante la imposibilidad de escoger la primera pauta, debemos pasar a la siguiente y así, consecutivamente: 1) que la eficiencia económica por sí sola dictaría aquel conjunto de derechos que favorece las opciones bien informadas entre los beneficios sociales y los costos sociales de obtenerlos, y entre los costos sociales y los costos sociales de evitarlos; 2) que ello implica, en ausencia de certeza respecto de si un beneficio vale sus costos para la sociedad, que el costo debería ser impuesto a la parte o actividad mejor situada para hacer tal análisis de costo-beneficio; 3) que en contextos particulares, como accidentes o contaminación, esto sugiere cargar los costos a la parte o actividad que puede evitarlos del modo más barato; 4) que en ausencia de certeza respecto de quién es esa parte o actividad, los costos deberían ser cargados a la parte o actividad que puede actuar con los menores costos de transacción en el mercado a fin de corregir un error en los derechos, induciendo a aquella parte que puede evitar los costos sociales de modo más barato a que lo haga, y 5), que desde que nos hallamos en un área en que por hipótesis los mercados no operan de modo perfecto —hay costos de transacción—, a menudo tendrá que adoptarse una decisión acerca de si son las transacciones de mercado o las regulaciones colectivas lo que con mayor probabilidad nos acerca al resultado óptimo de Pareto que el mercado "perfecto" alcanzaría.

El criterio de la eficiencia económica en la asignación de las titularidades no es el único aplicable, Calabresi y Melamed, también se refieren a las preferencias de distribución u objetivos distributivos. La asignación de derechos juega un rol fundamental en las preferencias distributivas de una determinada sociedad, ya que usualmente aquél al que se le asigna un conjunto de derechos por sobre otro, va a ser más rico que ese otro, ejemplifican estos autores indicando que "Una sociedad financieramente igualitaria que concede a los individuos el derecho a hacer ruido inmediatamente convierte al potencial bullicioso en alguien más rico que el ermitaño amante del silencio. Paralelamente, una sociedad que concede a una persona

obras versus el derecho a acceso a la cultura; el derecho a la víctima de un accidente a la reparación versus el derecho del causante del accidente a no reparar, etc.

inteligente el derecho a retener lo que su sagacidad le permite ganar implica una distribución de riqueza diferente de la adoptada por una sociedad que exige a cada uno de acuerdo a su capacidad relativa, pero da a cada uno según su deseo relativo. Uno puede ir más allá y considerar que una mujer hermosa o un hombre apuesto estarán mejor en una sociedad que concede a los individuos el derecho a la integridad física que en otra en la cual se concede a cualquiera el acceso a toda la belleza disponible."

Interesante resultan las ideas expuestas a propósito de la distribución de bienes de mérito, este tipo de bienes son ciertos derechos o titularidades que son asignadas a las personas porque la sociedad estima que debe maximizar las posibilidades de que los individuos gocen de a lo menos una mínima dote de estos bienes específicos, como por ejemplo, educación, vestuario, integridad física. Ahora bien, si la sociedad estima tal dote como esencial más allá de los deseos individuales, procederá, por supuesto, a convertir esa dote en algo inalienable. Bajo estas circunstancias, señalan Calabresi y Melamed, una sociedad que prefiere que las personas disfruten del silencio, o posean propiedad o gocen de integridad física, pero que no considere que los fundamentos de su preferencia son suficientemente fuertes como para que se justifique ignorar las preferencias opuestas, concederá tales derechos de acuerdo con la preferencia colectiva, aun cuando permita transarlos posteriormente. Cada vez que las transacciones para vender o adquirir derechos sean muy onerosas, tal decisión inicial de concesión de derechos será casi tan efectiva para asegurar que los individuos tendrán el bien de mérito como sería el transformar el derecho en algo inalienable.

Por último, dentro del concepto de otras razones de justicia, estos autores incluyen todos aquellos criterios que no caben ni dentro de la eficiencia ni de la distribución, mencionando dos en específico: el del mérito relativo de los intereses o necesidades de las personas (v.gr. el de aquellos que prefieren el ruido y el de aquellos que prefieren el silencio) y la congruencia de la asignación escogida o su aparente congruencia, con otros derechos dentro de la sociedad.

4.2. Reglas para regular y proteger derechos

Una vez asignadas las titularidades, el Estado debe efectuar una segunda elección, a saber: cómo proteger las asignaciones efectuadas. Esta elección se refiere al modo en que los

derechos serán protegidos y a la posibilidad de que un individuo pueda vender o transar un derecho. Calabresi y Melamed indican que existen tres reglas a este respecto; proteger los derechos asignados a través de la propiedad, la responsabilidad o la inalienabilidad. Resulta importante destacar que estas tres categorías son mixtas o, a lo menos, potencialmente mixtas, en el sentido que un determinado derecho, puede encontrarse protegido por dos de ellas o incluso por las tres[616]. De otra parte, el nivel de intervención del Estado varía en intensidad dependiendo de la regla de protección adoptada, siendo, por regla general, menor en el caso de la regla de propiedad, mayor en la regla de responsabilidad, y mayor aun en la de inalienabilidad, como se verá a continuación.

a) Regla de Propiedad: Un derecho es protegido por una regla de propiedad en la medida en que quien desea quitarle el derecho a su titular debe comprárselo en una transacción voluntaria, en la que el valor del derecho es aceptado por quien lo enajena, de manera que cada parte manifiesta cuánto vale el derecho para sí misma y se otorga al vendedor un veto si el comprador no ofrece lo suficiente. Esta es la forma de titularidad que da pie a la menor cantidad de intervención estatal: una vez decidida la titularidad original del derecho, ni el Estado ni la sociedad intentan decidir su valor.

Calabresi y Melamed establecen ciertas reglas según las cuales es correcto, desde un punto de vista de eficiencia económica, proteger las titularidades vía derechos de propiedad; así ocurrirá cada vez que los costos de transacción sean nulos o bajos, de manera que, aun cuando no existiese seguridad que el derecho asignado es el correcto, las partes transarán dejando el derecho en aquella que lo valúa más. No obstante lo anterior, todavía es posible utilizar el derecho de propiedad cuando existen costos de transacción significativos, en la medida en que se tenga certeza de quién puede evitar los costos de una manera más barata, así el criterio de eficiencia indica que la asignación de derechos se debe efectuar a favor de aquél que no puede evitar los costos a menor precio, de manera que la eficiencia

[616] Así indican Calabresi y Melamed en el artículo citado que "La casa de Taney puede estar protegida por una regla de propiedad en caso de que Marshall desee adquirirla, por una regla de responsabilidad cada vez que el gobierno pretenda expropiarla, y por una regla de inalienabilidad si Taney es alcohólico o incompetente."

económica se obtendrá sin transacciones mediante una asignación inicial de derechos correcta o dicho de otro modo, "las leyes e instituciones sociales más eficientes son las que asignan la carga del ajuste que obligan a hacer las externalidades a aquellos que pueden llevarlo a cabo con el menor costo posible.[617]"

b) Regla de Responsabilidad: Un derecho está protegido por una regla de responsabilidad cuando una persona puede destruir un derecho inicial y está dispuesta a pagar por él un valor objetivamente determinado por algún organismo del Estado y no por las propias partes, de manera que las reglas de responsabilidad implican un paso adicional de intervención estatal: no sólo se protegen los derechos, sino que se permite su transferencia o destrucción sobre la base de un valor determinado.

Se indica que se deberá utilizar la regla de la responsabilidad cada vez que no exista seguridad respecto de quién puede evitar el costo al menor valor, pues si existiera tal certidumbre, el costo de las reglas de responsabilidad (en esencia los costos de evaluar colectivamente los daños para todos los interesados, más el costo de la coacción contra todos aquellos que no están dispuestos a vender al valor colectivamente establecido) es innecesario.

c) Reglas de inalienabilidad: Un derecho es inalienable en la medida en que su transferencia está prohibida entre un comprador dispuesto y un vendedor también dispuesto. El Estado interviene no sólo para determinar quién posee inicialmente un derecho y la compensación que habrá de pagarse si éste se quita o destruye, sino que también para prohibir su venta bajo determinada o cualquier circunstancia.

Se señala por estos autores que la existencia de altos costos externos o externalidades lleva a que, en base a la eficiencia, se opte por proteger un derecho por una regla de inalienabilidad, siempre que los costos de transacción sean tan elevados que no permitan a las partes negociar, impidiendo que se adopte una regla de propiedad y que el valor objetivamente

[617] FRANK, Robert. op.cit. pág. 524.

determinado por el Estado, sea tan alto que nadie esté dispuesto a pagarlo, impidiendo que se adopte la regla de la responsabilidad. Otra supuesto para escoger la inalienabilidad como regla de protección de un derecho ocurre cuando los costos externos no se prestan para mediciones colectivas que sean aceptablemente objetivas y no arbitrarias debido a la imposibilidad de valorar un derecho (no monetarización). Esos costos externos muchas veces son llamados moralismos, ejemplo de ellos es el derecho inalienable a la libertad.

GLOSARIO

Asignación eficiente en el Sentido de Pareto: Asignación de los recursos en la que no es posible mejorar el bienestar de ninguna persona sin empeorar el de alguna otra.

Asimetría de información: Falla de mercado que se presenta cada vez que entre dos personas dispuestas a intercambiar, existe un desequilibrio tal de información que impide, en definitiva, el intercambio.

Beneficio marginal: El beneficio que recibe una persona de consumir una unidad adicional de un bien o servicio. Se mide como el monto máximo que una persona está dispuesta a pagar por una unidad más de un bien o servicio.

Beneficio marginal social: El beneficio marginal recibido por el comprador de un bien (beneficio marginal privado), más el beneficio marginal recibido por otros (beneficio externo).

Beneficios externos: Beneficios que recibe gente distinta al comprador del bien.

Bien económico: Es una mercancía capaz de proporcionar la satisfacción directa o indirecta de las necesidades humanas. Existen diferentes tipos de bienes económicos: de consumo, de inversión, bienes duraderos y no duraderos, bienes de capital y bienes intermedios.

Bien excluible: Bien de cuyo consumo se puede excluir a una persona.

Bien privado: Bien cuyo consumo es rival y excluible.

Bien público: Bien cuyo consumo no es rival ni excluible.

Bien rival: Bien cuyo consumo por parte de una persona reduce el consumo por parte de otra.

Competencia Perfecta: Modelo económico más utilizado. Se supone que hay un elevado número de compradores y vendedores de un bien cualquiera y que cada agente es un precio-aceptante.

Costo de oportunidad: Coste de utilizar los recursos para una determinada finalidad, medido por el beneficio al que se renuncia al no utilizarlos en su mejor uso alternativo. Costo de utilizar un recurso medido por el valor del mejor uso alternativo de ese recurso.

Costos de Transacción: Término que es utilizado por Coase para incluir todos los impedimentos de la negociación, como por ejemplo, descubrir con quién deseamos transar, informar a la gente que deseamos intercambiar y en qué términos, conducir negociaciones que lleven a un convenio, redactar el contrato, llevar a cabo la inspección necesaria para asegurarnos de que los términos del contrato se observan.

Costo marginal: Incremento del costo total al aumentar una unidad la cantidad producida.

Costo marginal social: El costo marginal en el que incurre el productor de un bien (costo marginal privado), más el costo marginal impuesto a otros miembros de la sociedad (costo externo).

Costos externos: Costos que no asume el productos del bien, sino alguien más.

Derechos de Propiedad: Especificación legal de la propiedad y de los derechos de los propietarios.

Discriminación de precios: Sistemas que pueden adoptar las empresas monopolistas o con gran poder de mercado para aumentar sus ingresos y beneficios. Ocurrirá siempre y cuando un comprador o vendedor pueda utilizar eficazmente su poder de mercado para separar los mercados y adoptar una política de precios distinta en cada uno. Así por ejemplo, las líneas aéreas discriminan sus precios (clase turista, ejecutiva, primera) de acuerdo a la disposición a pagar de los pasajeros por mayor o menor comodidad al viajar en avión.

Disposición a pagar: Cantidad máxima que pagaría un consumidor por adquirir un determinado bien.

Economía de mercado: Economía en la que la asignación de recursos se realiza por medio de las decisiones descentralizadas de muchas empresas y familias, conforme interactúan en el mercado de bienes y servicios.

Economía: Ciencia que estudia el modo en que la sociedad gestiona sus recursos escasos. Busca lograr una asignación eficiente de dichos recursos entre sus empleos alternativos con el fin de lograr ciertos objetivos.

Eficiencia: Propiedad por la cual la sociedad aprovecha de la mejor manera posible sus recursos escasos.

Equidad: Propiedad según la cual la prosperidad económica se distribuye de forma igualitaria (equitativa) entre los miembros de la sociedad. Existe cuando los recursos se asignan de tal forma que no es posible aumentar ninguna actividad sin reducir alguna otra.

Equilibrio: Situación en la que no existe ninguna tendencia al cambio porque se cumplen los planes de compra y venta de demandantes y oferentes, de modo que el mercado se vacía.

Externalidad: Consecuencias que la acción de un agente económico tiene sobre el bienestar de otro y que no es tenido en cuanta por la conducta normal del mercado. Resultado de una acción que no es absorbida por la persona que toma las decisiones. Si existen costos externos, las personas que toman las decisiones sobreexplotarán la actividad, debido a que ellos no soportan todo el costo; la contaminación es el ejemplo clásico. Si existen beneficios externos, las personas que toman las decisiones subexplotarán la actividad, debido a que ellos no obtienen todo el beneficio. La información a menudo se asocia con beneficios externos. La existencia de externalidades puede llevar al fracaso en el mercado.

Falla de Mercado: Alguna condición que causa que los mercados entreguen un desempeño subóptimo. En otras palabras, situación en la que el mercado por sí solo no asigna eficientemente

los recursos. Las causas clásicas son el poder de mercado, externalidades, e información asimétrica.

***Free-Rider*:** Consumidor de un bien no exclusivo, que no paga por éste con la esperanza de que otros consumidores lo paguen.

Información asimétrica: Información conocida sólo por una parte de la transacción. La existencia de información asimétrica puede causar una "falla de mercado" debido a que las partes que saben que tienen menos información no estarán dispuestas a comerciar ni intercambiar bienes o servicios. El mercado resultante es llamado *mercado de limones*.

Ingreso marginal: Aumento del ingreso total generado al vender una unidad adicional de producción.

Mejoramiento paretiano: Cuando la utilidad o beneficio de un agente económico aumenta sin que por ello disminuya la utilidad o beneficio de ningún otro agente.

Mercado de Limones (*Lemons Market*): Falla de mercado asociada con información asimétrica, donde sólo los vendedores de productos de baja calidad existen.

Microeconomía: Rama de la economía que estudia cómo los agentes individuales (las empresas y los consumidores) toman decisiones y su interacción en el mercado.

Modelo: Representación simplificada de la realidad con la que se pretende explicar aquello que se considera relevante dentro de esa realidad.

Monopolio: Tipo de mercado en el que hay un solo productor u oferente.

***Opt-In* y *Opt-Out*:** 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.

Poder de mercado: Medida de la capacidad de una empresa para influir sobre el precio en un mercado. Una forma de medir el poder de mercado es calculando la diferencia entre el precio y el coste marginal.

Precio-aceptante: Agente económico que toma decisiones basándose en el supuesto de que éstas no influyen en los precios vigentes de mercado.

Precio de equilibrio: Precio al que se igualan cantidad demandada y cantidad ofrecida,

Riesgo moral: Influencia de la cobertura de un seguro en las decisiones de los individuos de realizar actividades que puedan altera la probabilidad de incurrir en pérdidas.

Selección adversa: Situación en la que los mercados tienen dificultades de funcionamiento debido a que sólo consumidores con características específicas entran el mercado. Esto es un problema común en los mercados de seguro, donde sólo los consumidores con mayor probabilidad de necesitar seguros, es decir, aquellos con mayor riesgo, comprará. De igual manera, los prestamistas no quieren atraer créditos riesgosos. Un *mercado de limones* es causado por la selección adversa. Es un ejemplo de un problema asociado con información asimétrica.

Teorema de Coase: Resultado atribuible a R. Coase: si los costos de negociación (transacción) son cero, es posible asignar eficientemente los recursos en presencia de externalidades por medio de una negociación entre las partes afectadas.

Utilidad: El placer o la satisfacción de una necesidad que las personas obtienen de su actividad económica.

BIBLIOGRAFIA CONSULTADA

TRATADOS, INSTRUMENTOS E INFORMES INTERNACIONALES

Declaración Universal de Derechos Humanos, Naciones Unidas, 1948. Art. 12

Pacto Internacional de Derechos Civiles y Políticos. Asamblea General de las Naciones Unidas, 1966. Art. 17.

Convención Americana sobre Derechos Humanos, 1962. Art. 11

Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Octubre 1995.

Directiva 97/66/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Diciembre 1997

Directiva 2002/58/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Julio 2002.

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, del Consejo de Europa. Agosto 1981.

Principios rectores para la reglamentación de los ficheros computarizados de datos personales Asamblea General de las Naciones Unidas. Resolución 45/95 de 14 de diciembre de 1990.

The guidelines on the protection of privacy and transborder flows of personal data. OCDE 1980.

Principios de Puerto Seguro. Federal Trade Commission. Julio de 2000.

LEGISLACIÓN, ACTOS ESTATALES Y OTROS DOCUMENTOS:

ALEMANIA. 2002. Bundesdatenschutzgesetz (BDSG).

ARGENTINA. 2000. Ley 25.326 argentina de Protección de Datos.

ARGENTINA. Constitución Argentina (art. 43 inc. 3°).

BRASIL. Constitución Brasilera (art. 5 LXXII).

COLOMBIA. Constitución Colombiana (art. 15).

DINAMARCA. 2000. Lov N° 429 af 31 maj 2000 som aendret ved lov N° 280 af 25 april 2001.

ECUADOR. Constitución Ecuatoriana. (art. 94 inc. 2°).

ESPAÑA. 1999. Ley Orgánica 15/99, de Protección de Datos de Carácter Personal.

ESPAÑA. 1992. Ley Orgánica 5/92, de Regulación del Tratamiento Automatizado de Datos.

ESPAÑA. 1994. Real Decreto 1332/94, sobre reglamentación de la LORTAD.

ESTADOS UNIDOS. 1984. The Cable Communications Policy Act. U.S.C. 551 (1994).

ESTADOS UNIDOS. 1984. The Video Privacy Protection Act. U.S.C. 551 (1994).

ESTADOS UNIDOS. 1984. 2003. “Fair and Accurate Credit Transactions Act of 2003" To amend the Fair Credit Reporting Act, to revent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes. Public Law 108-159. 108th Congress.

ESTADOS UNIDOS. *1974.* Privacy Act. USC Sec. 552ª.

ESTADOS UNIDOS. *1978. Right to Financial Privacy.* 12 U.S.C. 3401Ç

ESTADOS UNIDOS. *1978 Electronic Fund Transfer Act* (15 U.S.C. Sec. 1601 et seq.)

ESTADOS UNIDOS. *1986 Electronic Communication Privacy Act.* 18 U.S.C. § 2703(d)

ESTADOS UNIDOS. *1988.* Computer Matching and Privacy Protection Act of 1988. (5 U.S.C. 552a(o) et seq.)

ESTADOS UNIDOS. *1988. Video Privacy Protection Act.* (18 U.S.C. § 2710)

ESTADOS UNIDOS 2001. USA Patriot Act of 2001: Section 358 to permit the disclosure of financial information to any intelligence or counterintelligence agency in any investigation related to international terrorism.

GRECIA. 1997. Ley 2.472 de protección de las personas respecto al tratamiento de datos de carácter personal.

GUATEMALA. Constitucón Guatamalteca (art. 31).

INGLATERRA. 1998. Data Protection Act.

ITALIA. 1996. Legge N° 675, tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Nicaragua. Constitución Nicaragüense. (art. 26 N° 4).

PARAGUAY. Constitución Paraguaya (art. 135).

PORTUGAL. 1998. Ley 67/98 de 26 de octubre de 1998 sobre la protección de datos personales.

URUGUAY. 2004. Ley 17.838 de Protección de datos personales para ser utilizados en informes comerciales y acción de hábeas data.

VENEZUELA. Constitución Venezolana (art. 28).

LEGISLACIÓN NACIONAL

Constitución Política de la República de Chile. 1980.

Código Civil.

Ley N° 19.812. 2002. Modifica la Ley 19.628 sobre Protección de la Vida Privada.

Ley 19.628 sobre Protección de la vida privada. Agosto 1999.

Ley N° 19.891. 2003. Crea el consejo nacional de la cultura y las artes y el fondo nacional de desarrollo cultural y las artes.

Decreto Ley N° 645 sobre el Registro Nacional de Condenas. Octubre 1925.

D.F.L.1. 2003. Fija el texto refundido, coordinado y sistematizado del Código del Trabajo.

Decreto con Fuerza de Ley N°3 que fija texto refundido, sistematizado y concordado de la Ley General de Bancos y de otros cuerpos legales que indica. Diciembre 1997

Decreto Supremo de Hacienda N° 950. 1928.

SITIOS WEB

ASOCIACIÓN DE BANCOS E INSTITUCIONES FINANCIERAS A.G. Sinacofi. 2005 [en línea] < http://www.abif.cl/menu-superior/filiales/sinacofi.htm> [consulta: 16 febrero 2005].

ASOCIACIÓN ESPAÑOLA DE COMERCIO ELECTRÓNICO. CÓDIGO DE ÉTICA. 2005 [en línea] < www.aece.org/docs/codigo.pdf> [consulta: 18 febrero 2005].

ASOCIACIÓN MEXICANA DE LA INDUSTRIA PUBLICITARIA Y COMERCIAL EN INTERNET. CÓDIGO DE ÉTICA. 2005 [en línea] < http://www.amipci.org.mx/amipci/codigo_de_etica.html > [consulta: 18 febrero 2005].

BOLETIN COMERCIAL. CAMARA DE COMERCIO DE SANTIAGO. 2006. [en línea] <http://www.boletincomercial.cl/html/que_es_bic.htm> [consulta: 14 febrero 2006].

CÁMARA DE COMERCIO DE SANTIAGO Economía Digital. 2000 [en línea] <http://www.ccs.cl/html/actualizar/Estudios/edigtal.PDF > [consulta: 16 febrero 2005].

CAMARA DE COMERCIO DE SANTIAGO. Código de buenas prácticas. [en línea] <http://www.ccs.cl/html/codigo_buenas_practicas/inicio-cbp.htm> [consulta: 1 marzo 2006].

CONSEJO DE AUTORREGULACIÓN Y ÉTICA PUBLICITARIA. CÓDIGO DE ÉTICA. 2005 [en línea] < http://www.conar.cl/p4_portada/antialone.html?page=http://www.conar.cl/p4_portada/site/artic/20031124/pags/20031124163705.html > [consulta: 18 febrero 2005].

DATARENT. Cláusula contractual datarent. 2005 [en línea] <http://www.datarent.cl/Inicio/Clausula.htm > [consulta: 15 febrero 2005].

DATARENT. Preguntas Frecuentes acerca de datarent. http://www.datarent.cl/Inicio/Faq.htm> [consulta: 15 febrero 2005].

DECLARACIÓN CONJUNTA NIC CHILE- ACEPTA.COM. 2001. [en línea] http://www.nic.cl/anuncios/2001-05-15.html [consulta: 15 febrero 2006].

DICCIONARIO DE TÉRMINOS INFORMÁTICOS [en línea] http://www.moheweb.galeon.com/diccinformatic.htm#C [consulta: 29 marzo 2005].

DICOM HOME. 2006. [en línea] <https://www.dicom.cl/com/com.01/pag/p.com.com.cons-dir-pers-p.htm>> [consulta: 15 febrero 2006].

DICOM. Dicomguías. 2005 [en línea] <https://www.dicom.cl/dhom/pag/p.hom.000.f-productos.htm> [consulta: 29 marzo 2005].

ELECTRONIC PRIVACY INFORMATION CENTER. [EN LÍNEA] <http://www.epic.org/privacy/consumer/states.html#wash> [consulta: 25 marzo 2005]

EL MERCURIO DE VALPARAÍSO. 2002. [en línea] <http://www.mercuriovalpo.cl/site/edic/20021129205118/pags/20021130010226.html> [consulta: 29 marzo 2005].

ELMERCURIO.COM 2006. [en línea] <http://www.economiaynegocios.cl/noticias/noticias.asp?id=85255> [consulta: 25 marzo 2006].

ELMERCURIO.COM 2006. [en línea] <http://diario.elmercurio.com/2006/03/20/editorial/tribuna/noticias/39103DB6-DE1A-4A4E-A144-2C429C717E71.htm> [consulta: 25 marzo 2006].

EMOL EL MERCURIO. El negocio de las temidas bases de datos de incumplimientos comerciales. 2003 [en línea] <http://www.economiaynegocios.cl/tus_finanzas/tus_finanzas.asp?id=568&numero=14> [consulta: 14 febrero 2005].

EARTHLINK. 2005. [en línea] http://www.earthlink.net/spyaudit/press/ [consulta: 29 marzo 2005].

EQUIFAX. 2006. [en línea] <https://www.dicom.cl/dic/hom.01/pag/p.dic.hom.mas-productos-personas.htm#> [consulta: 14 febrero 2006].

MAPCITY. 2004-2005. [en línea] <http://www1.mapcity.com/empresa_geo.php> [consulta: 16 febrero 2005].

REVISTA QUE PASA. Chilenos al desnudo. 2000. [en línea] <http://64.233.161.104/search?q=cache:0Tl29o0NZJ:www.quepasa.cl/revista/1511/36.html+%22datos+personales%22+%22marketing+directo%22&hl=es > [consulta: 16 febrero 2005].

SERVICIO REGISTRO CIVIL E IDENTIFICACION. 2006. [en línea] <https://www.registrocivil.cl/OficinaInternet/servlet/MuestraPagina?contexto=1&pagina=/Institucion/convenio_con_empresas/ConveniosEmpresasInstituciones.html> [consulta: 16 febrero 2006].

SERVICIO REGISTRO CIVIL E IDENTIFICACION. CONSULTA. 2005. [en línea] <http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html> [consulta: 15 febrero 2006]

SERVICIO REGISTRO CIVIL E IDENTIFICACION. 2006. [en línea] <https://www.registrocivil.cl/OficinaInternet/servlet/MuestraPagina?contexto=1&pagina=/Institucion/convenio_con_empresas/ConveniosEmpresasInstituciones.html> [consulta: 16 febrero 2006].

SISTEMA NACIONAL DE COMUNICACIONES FINANCIERAS. 2006. [en línea] <http://www.sinacofi.cl/marco_legal.asp> [consulta: 14 febrero 2006].

SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS [en línea] <http://www.sbif.cl/NormasSBIF/Bancos/C2544B.pdf> [consulta: 9 de Mayo 2003]

SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS A.G. 2005 [en línea] <http://www.sbif.cl/sbifweb/servlet/AtencionPublico?indice=1.2.1.1&idContenido=996> [consulta: 16 febrero 2005].

Servicio de Registro Civil e Identificaciones [en línea] http://www.registrocivil.cl/ofinternet/doAction?actionName=viewMenuCertificados&modoEnvio=onLine [consulta: 12 enero 2004].

DOCTRINA

ABRIL, G. 1997. Teoría general de la información. Madrid, Ediciones Cátedra S.A. 344p.

ALESSANDRI, A. s.a. Derecho Civil. De los bienes. Santiago de Chile, Editorial Lex. Tomo segundo.

ALVAREZ-CIENFUEGOS, J. M. 1999. La defensa de la intimidad de los ciudadanos y la tecnología informática. Pamplona, Editorial Aranzadi S.A. 161p.

ARENAS, M. F. 2002. Nuevas tecnologías y sistemas de información: contextos y paradigmas. [en línea] < http://www.redcom.org/CCC/foro6_arenas.htm> [consulta: 05 junio 2005].

BAINBRIDEGE, D. 2005. Data Protection Law. 2ª ed. Great Britain, xpl publishing. 328p. pág. 62.

BAJO, J. 2004. Derecho comunitario sobre protección de datos. EN: GOMEZ, M. Derecho a la intimidad y nuevas tecnologías. Madrid, Consejo General del Poder Judicial. pp. 45-76.

BERTELSEN, R. 2001. Datos personales: propiedad privada, libre iniciativa particular y respeto a la vida privada. En Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5. pp. 113-129

BULLARD, A. No se lo digas a nadie. Se puede vender el derecho a la privacidad en el mercado. Revista Ius et Veritas. Año X. (17).

CALABRESI, G. y MELAMED, D. *"Property Rules, Liability Rules, and Inalienability: One View of the Cathedral"*, en Harvard Law Review, Vol. 85, Nº 6, 1972, pp. 1.089-1.128.

CARDONA D. 2002. Economía o sociedad de la información. [en línea] <http://dsi.esade.edu/dcardona/CV/publicac.htm> [consulta: 05 junio 2005].

CARRILLO, M. 2003. El derecho a no ser molestado. Información y vida privada. Navarra, Aranzadi. 172p.

CASTELLS, M. 1999. La era de la información: economía, sociedad y cultura. Madrid, Siglo veintiuno de España editores. Vol.1.

CASTELLS, M. 2002. La dimensión cultural de Internet. [en línea] <http://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.htm> [consulta: 25 junio 2005].

CAVOUKIAN, A. 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] 37p.

CERDA, A. 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.

COASE, R. "*The Problem of Social Cost*", Journal of Law and Economics, vol. 3, 1960 p. 1.

COHEN, J. 2000. Examined Lives: Informational privacy and the subject as object. Stanford Law Review 52: 1373-1437.

COLEMAN, J. 1980. Efficiency, utility and wealth maximization. EN: Hofstra Law Review, vol.8, Nº 3

COLOMA, G. 1999. Apuntes para el Análisis Económico del Derecho Privado Argentino, CEMA Working Papers Universidad del CEMA. 156p.

COOTER, R. y ULEN, T. 1999. Derecho y economía. 1ª reimpresión. México D.F., Fondo de Cultura Económica. 686p

DAVARA, M. 1996. De las autopistas de la información a la sociedad virtual. Pamplona, Editorial Aranzadi S.A. 191p.

DAVARA, M. 1997. Manual de Derecho Informático. Madrid, Editorial Aranzadi. 396 p. pág. 66. BAUTISTA R. 1993. Protección Jurídica de datos personales automatizados. Madrid, Editorial Colex. 272p. pág. 96.

DAVARA, M. 1998. La protección de datos en Europa. Principios, derechos y procedimiento. Madrid, Grupo Asnef Equifax. 204p.

DE LA MAZA, I. 2002. Privacidad y comercio electrónico. EN: DE LA MAZA, I. Derecho y tecnologías de la información. Fundación Fernando Fueyo Laneri. Escuela de Derecho. Universidad Diego Portales. pp. 265-279.

ELLIOT, PH. 1986. Intellectuals, the "information society" and the disappearence of the public sphere.

FERGUSON, E. 1969. Teoría Microeconómica. México, Fondo de Cultura Económica. 456p.

FLORES, A. Sociedad de la información. [en línea] <http://www.monografias.com/trabajos15/sociedad-informac/sociedad-informac.shtml> [consulta: 30 septiembre 2005].

FLORIANO, C. 1998. Derecho y economía. Una aproximación al análisis económico del derecho. Badajoz, Universidad de Extremadura. Servicio de publicaciones. 190p.

FRANK H. R. 2001. Microeconomía y conducta. 4ª ed. Madrid, Mc Graw-Hill. 595p.

FROOMKIN, M. 2000. The Death of privacy? Stanford Law Review. 52: 1461-1543.

GALÁN, M. 2005. Intimidad. Nuevas dimensiones de un viejo derecho. Madrid, Editorial Centro de Estudios Ramón Areces S.A. 278p.

GARCÍA, L. 1992. Reflexiones sobre la intimidad como límite de la libertad de expresión. EN: Estudios sobre el derecho a la intimidad. Madrid, Editorial Tecnos. pp. 15-35.

GELLMAN, R. Does privacy law work? EN: Philip E. Agre and Marc Roenberg editors, Technology and Privacy: The new landscape. (Massachusetts Institute of Technology, 1997), p.203.

GHILIANI, L. 1998. Datos personales: propiedad y derecho al uso. [en línea] <http://www.it-cenit.org.ar/Publicac/PeopleBases/Recopilac/Recopilac2.htm> [consulta: 24 noviembre 2003]

GONZÁLEZ, F. 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.

GOZAINI, O. 2001. Hábeas data. Protección de datos personales. Doctrina y jurisprudencia. Buenos Aires, Rubinzal-Culzoni. 526p.

GRIMALT, P. 1999. La responsabilidad civil en el tratamiento automatizado de datos personales. Granada, Editorial Comares. 382p.

GUERRERO, J. 1997. La empresa privada y la magistratura ante la acción de hábeas data. Revista Ius et Praxis. Universidad de Talca. Año 3. N° 1: 209-218

HARRIS, P.R. The european perspective: is data protection value for money? [en línea] <http://26konferencja.giodo.gov.pl/data/resources/HarrisR_paper.pdf> [consulta: 19 marzo 2006].

HASSEMER, W. y CHIRINO, A. 1997. El derecho a la autodeterminación informativa y los restos del procesamiento automatizado de datos personales. Buenos Aires, Editores del Puerto s.r.l. 238p.

HEREDERO, M. 1997. La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Madrid, Editorial Aranzadi. 372 p.

HERRÁN, O. A. 2002. El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales. Madrid, Dykinson. 388 p.

HERRERA, R. 2001. Digitalización y convergencia: el nuevo entorno de las telecomunicaciones. [en línea] <http://www.adi.cl/pdf/digyconv.pdf> [consulta: 16 febrero 2005].

HERRERA, R. 2001. La protección de datos personales como garantía básica de los derechos fundamentales. Revista de Derecho Público, de la Agrupación de Abogados de la Contraloría General de la República, Año N°2, (5)

HERRERA, R. 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].

HUI, K. Y PNG, I. 2005. The economics of privacy. Handbook of information systems and economics. Elsevier, Terry Hendershott ed.

JAÑA, W. Análisis legal comparativo de la protección de datos personales a nivel latinoamericano. (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Facultad de Derecho, Universidad de Chile. 2003. 516h.

JIJENA, R. 2001. La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos. En Cuadernos de Extensión Jurídica (U. de Los Andes) N° 5. pp. 85-111.

KANG, J. 1998. Information privacy in cyberspace transactions. Stanford Law Review 50: 1193-1294.

KARAS, S. 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].

KITCH, E. 1983. The intellectual foundations of law and economics. En: Journal of legal education, vol.33, N° 2. pág. 183-209.

LAUDON ,K. 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].

LESSIG, L. 2001. El código y otras leyes del ciberespacio. Madrid, Taurus. 544p.

LITMAN, J. 2000. Information privacy/information property. Stanford Law Review 52: 1283-1313.

MARCELLA, A. J. y STUCKI, C. 2003. Privacy Handbook. Guidelines, exposures, policy implementation and internacional issues. New Jersey, John Wiley & Sons, Inc. 357p.

MARIO LOSANO "et al". Madrid, Centro de Estudios Constitucionales. 213p.

MASUDA, Y. 1984 La sociedad informatizada como sociedad post-industrial. Madrid, Tecnos. 171p.

NOAM, E. 1997. Privacy and self-regulation: Markets for electronic privacy. [en línea] Privacy and Self-Regulation in the information age. U.S. Department of Commerce, June 1997. <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1B> [consulta: 18 febrero 2006].

NOTT, L. 2003. Financial privacy: an economic perspective. Report for Congress order code RL31758 [en línea] <HTTP://www.epic.org/privacy/glba/RL31758.pdf> [consulta: 02 febrero 2005]

NOVOA, E. 1979. Derecho a la vida privada y libertad de información. Un conflicto de derechos. 5ª ed. México, Siglo veintiuno editores. 224p.

PALAZZI, P. La transmisión internacional de datos personales y la protección a la privacidad. 2002. Buenos Aires, Ad-hoc. 416p.

PÉREZ-LUÑO, A. 1992. Intimidad y protección de datos personales: del habeas corpus al habeas data. EN: Estudios sobre el derecho a la intimidad. Madrid, Editorial Tecnos. pp. 36-45.

PEREZ-LUÑO, A. 1996. Manual de informática y derecho. Barcelona, Ariel Derecho. 222p.

PORAT, M. 1997. The information economy: definitions and measurement OT Special Publication 77-12 (1), US Department Of. Commerce.

POSNER, R. 1981. The economics of justice. Cambridge, Harvard University Press. 415p.

POSNER, R. 1998. El análisis económico del derecho. México D.F. Fondo de Cultura Económica. 682p.

POSNER, R. 1999. Orwell versus Huxley: Economics, Technology, Privacy and Satire. John M.Olin Law & Economics Working Paper. The Law School University of Chicago. (89): 1-35.

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].

PUCCINELLI, O. 1999. El hábeas data en indoiberoamérica. Santa Fé de Bogotá, Editorial Temis. 607p.

RIANDE, N. La desprotección de los datos personales. [en línea] <http://infoleg.mecon.gov.ar/basehome/noticias/riandejuarez-30-4.htm> [consulta: 24 noviembre 2003].

RIBAS, J. 2001. Riesgos Legales en Internet, especial referencia a la protección de los datos personales. EN: Derecho de Internet. Madrid, Ed. Aranzadi.

ROEMER, A., 1994. Introducción al análisis económico del derecho. México D.F. Fondo de Cultura Económica. 114p.

ROSE, E. 2005. Data users versus data subjects: Are consumers willing to pay for property rights to personal information? Proceedings of the 38th Annual Hawaii International Conference On System Sciences.

RUBIN, H. P. y LENARD, M. T. 2001. Privacy and the comercial use of personal information. Washington DC, The Progress & Freedom Foundation. 92p.

RUIZ, A**.** 1999. Los datos de carácter personal: concepto, requisitos de circulación, procedimientos, normativa y formularios. Barcelona, Bosch. 208p.

NICHOLSON, W. 1997. Teoría microeconómica: principios básicos y aplicaciones. Madrid, McGraw-Hill, 1997. 599p.

SAMUELSON, P y NORDHAUS, W. 2002. Economía. 17a ed. Madrid, McGraw-Hill. 387p.

SAMUELSON, P. 2000. Privacy as intellectual property? Stanford Law Review 52: 1125-1171.

SCHWARTZ, P. 2004. Property, privacy, and personal data. Harvard Law Review. 117: 2056-2128

SHOLTZ, P. 2001. Transaction costs and the social costs of online privacy. [en línea] First Monday. Vol. 6. number 5. http://firstmonday.org/issues/issue6_5/sholtz/index.html [consulta: 10 febrero 2005].

SOLOVE, D. 2001. Privacy and power: Computer databases and metaphors for information privacy. Stanford Law Review. 53: 1393-1462

SUÑÉ, E. 2000. Tratado de Derecho Informático. Introducción y protección de datos personales. Madrid, Servicio publicaciones facultad de derecho Universidad Complutense de Madrid. Vol.1.

SWIRE, P. 1997. Markets, self regulation, and government enforcment in the protection of personal information. [en línea] Privacy and Self-Regulation in the information age. U.S.

Department of Commerce, June 1997. <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm> [consulta: 18 febrero 2006].

TAYLOR, C. 2004. Privacy and information acquisition in competitive markets. [en línea] http://www.econ.duke.edu/Papers/Other/Taylor/privacy.pdf [consulta: 18 junio 2005]. pág. 1.

THAYER, L. 1975. Comunicación y sistemas de comunicación. Barcelona, Península.

THEORY OF TRANSACTIONS PRIVACY. 2000. Por CHARLES KAHN "et al". Federal Reserve Bank of Atlanta, Working Paper Series 2000-22. 27p.

VARIAN, H. 1996. Economic aspects of personal privacy. [en línea] <http://www.sims.berkeley.edu/~hal/Papers/privacy/> [consulta: 02 febrero 2005].

VERDUGO, M; PFEFFER, E.; NOGUEIRA, H. 1997. Derecho Constitucional. Santiago, Editorial Jurídica de Chile. 371p.

WARREN, S. y BRANDEIS, L. 1890. The right to privacy. Harvard Law Review. vol. IV, num 5.

WELLS, A. 1994. Who owns information. New Cork, Basic Books. 241p.