



Universidad de los Andes
Facultad de Derecho

Tratamiento de datos personales y protección de la vida privada

**ESTUDIOS SOBRE
LA LEY N° 19.628
SOBRE PROTECCIÓN DE DATOS
DE CARÁCTER PERSONAL**

**RAÚL BERTELSEN REPETTO
HERNÁN CORRAL TALCIANI
FRANCISCO GONZÁLEZ HOCH
RONY JARA AMIGO
RENATO JIJENA LEIVA
RAMIRO MENDOZA ZÚÑIGA
FELIPE VIAL CLARO**

**Jorge Wahl Silva
EDITOR**



2001

CUADERNOS DE EXTENSIÓN JURÍDICA 5



Universidad de los Andes

Facultad de Derecho

Tratamiento de datos personales y protección de la vida privada

**ESTUDIOS SOBRE LA LEY N° 19.628 SOBRE PROTECCIÓN
DE DATOS DE CARÁCTER PERSONAL**

Raúl Bertelsen Repetto

Hernán Corral Talciani

Francisco González Hoch

Rony Jara Amigo

Renato Jijena Leiva

Ramiro Mendoza Zúñiga

Felipe Vial Claro

Jorge Wahl Silva

EDITOR

CUADERNOS DE EXTENSIÓN JURÍDICA 5 (2001)

RAÚL BERTELSEN REPETTO, HERNÁN CORRAL TALCIANI
FRANCISCO GONZÁLEZ HOCH, RONY JARA AMIGO,
RENATO JIJENA LEIVA, RAMIRO MENDOZA ZÚÑIGA, FELIPE VIAL CLARO

CIP - Universidad de los Andes

Tratamiento de datos personales y protección de la vida privada:
estudios sobre la ley 19.628 sobre protección de datos de carácter
personal / Raúl Bertelsen Repetto ... [et al.]; Jorge Wahl Silva
editor. – (Cuadernos de Extensión Jurídica; 5)
Incluye notas bibliográficas.

1.- *Hábeas Data* – Chile. 2.- Protección de Datos – Aspectos
Jurídicos – Chile. 3.- Chile. Ley No. 19.628. I.- Bertelsen Repetto,
Raúl. II.- Wahl Silva, Jorge Adolfo, ed. III.- s,

CDD 21
342.830858 2002 RCA2

ISBN: 956-7160-21-X
Registro de Propiedad Intelectual Inscripción N° 126.218

No está permitida la reproducción parcial o total de este libro, o de alguna de sus partes, formatos
o portadas, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier
medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso
previo del titular de la propiedad intelectual.

© 2001 Universidad de los Andes
© Jorge Wahl Silva

Cuadernos de Extensión Jurídica
Ediciones Universidad de los Andes
Av. San Carlos de Apoquindo 2200, Las Condes, Santiago de Chile.

Diseño: Carolina Varela

Impresión
Andros Impresores

Impreso en Santiago de Chile – Printed in Santiago of Chile

RAÚL BERTELSEN REPETTO

Doctor en Derecho por la Universidad de Navarra (España)
Profesor Derecho Constitucional
Universidad de los Andes

HERNÁN CORRAL TALCIANI

Doctor en Derecho por la Universidad de Navarra (España)
Profesor de Derecho Civil
Universidad de los Andes

FRANCISCO GONZÁLEZ HOCH

Máster en Derecho por la Universidad de Harvard (EE.UU.)
Profesor de Derecho Civil
Universidad de Chile

RONY JARA AMIGO

Máster en Derecho por la Universidad de Duke (EE.UU.)
Profesor de Derecho Comercial
Universidad de los Andes

RENATO JIJENA LEIVA

Diplomado en Derecho Informático
por la Universidad de Zaragoza (España)
Profesor de Derecho Informático y del Diplomado en
E-Business de la Universidad de Chile

RAMIRO MENDOZA ZÚÑIGA

Profesor de Derecho Administrativo

Universidad de los Andes

P. Universidad Católica de Chile

FELIPE VIAL CLARO

Máster en Derecho por la Universidad

de Southampton (Inglaterra)

Profesor de Derecho Civil

Universidad de los Andes

PRÓLOGO	11
PRESENTACIÓN DEL EDITOR	17
LA LEY Nº 19.628 SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL UNA VISIÓN GENERAL <i>Felipe Vial Claro</i>	
I. Ámbito de aplicación	23
II. Marco regulatorio del tratamiento de datos personales	25
III. Principios rectores del desarrollo de la actividad de tratamiento organizado de datos personales	26
IV. Infracciones y sanciones	34
V. Vigencia	36
DE LOS DERECHOS DE LAS PERSONAS SOBRE LOS RESPONSABLES DE BANCOS DE DATOS: EL <i>HÁBEAS</i> <i>DATA</i> CHILENO <i>Hernán Corral Talciani</i>	
I. Introducción	39
II. Derechos legalmente reconocidos	42
III. Condiciones de ejercicio de los derechos ...	46
IV. Excepciones	50
V. El amparo digital o <i>hábeas data</i>	50
VI. Responsabilidad civil y derecho a la indemnización de perjuicios	55
VII. Derechos de los titulares de datos y la protección a la vida privada	57

RÉGIMEN DE LOS DATOS DE CARÁCTER ECONÓMICO,
FINANCIERO, BANCARIO O COMERCIAL
EN LA LEY N° 19.628
Rony Jara Amigo

I.	Introducción	61
II.	Algunos conceptos económicos y constitucionales básicos	61
III.	Experiencia del derecho y doctrina comparada y de la jurisprudencia nacional	66
IV.	Análisis de algunos elementos fundamentales de la ley N° 19.628	70
V.	Algunos problemas y posibles soluciones ..	77
VI.	Conclusiones	82

LA LEY CHILENA DE PROTECCIÓN DE DATOS
PERSONALES, UNA VISIÓN CRÍTICA DESDE EL PUNTO DE
VISTA DE LOS INTERESES PROTEGIDOS
Renato Jijena Letwa

I.	Introducción	85
II.	La protección de datos personales o nominativos y el <i>hábeas data</i> . Planteamientos doctrinarios y Derecho Comparado	86
III.	El procesamiento o "tratamiento" computacional de datos personales o nominativos en Chile. Los antecedentes sobre solvencia patrimonial.....	91
IV.	Análisis de la ley aprobada	93

DATOS PERSONALES: PROPIEDAD PRIVADA,
LIBRE INICIATIVA PARTICULAR Y RESPETO A LA
VIDA PRIVADA
Raúl Bertelsen Repetto

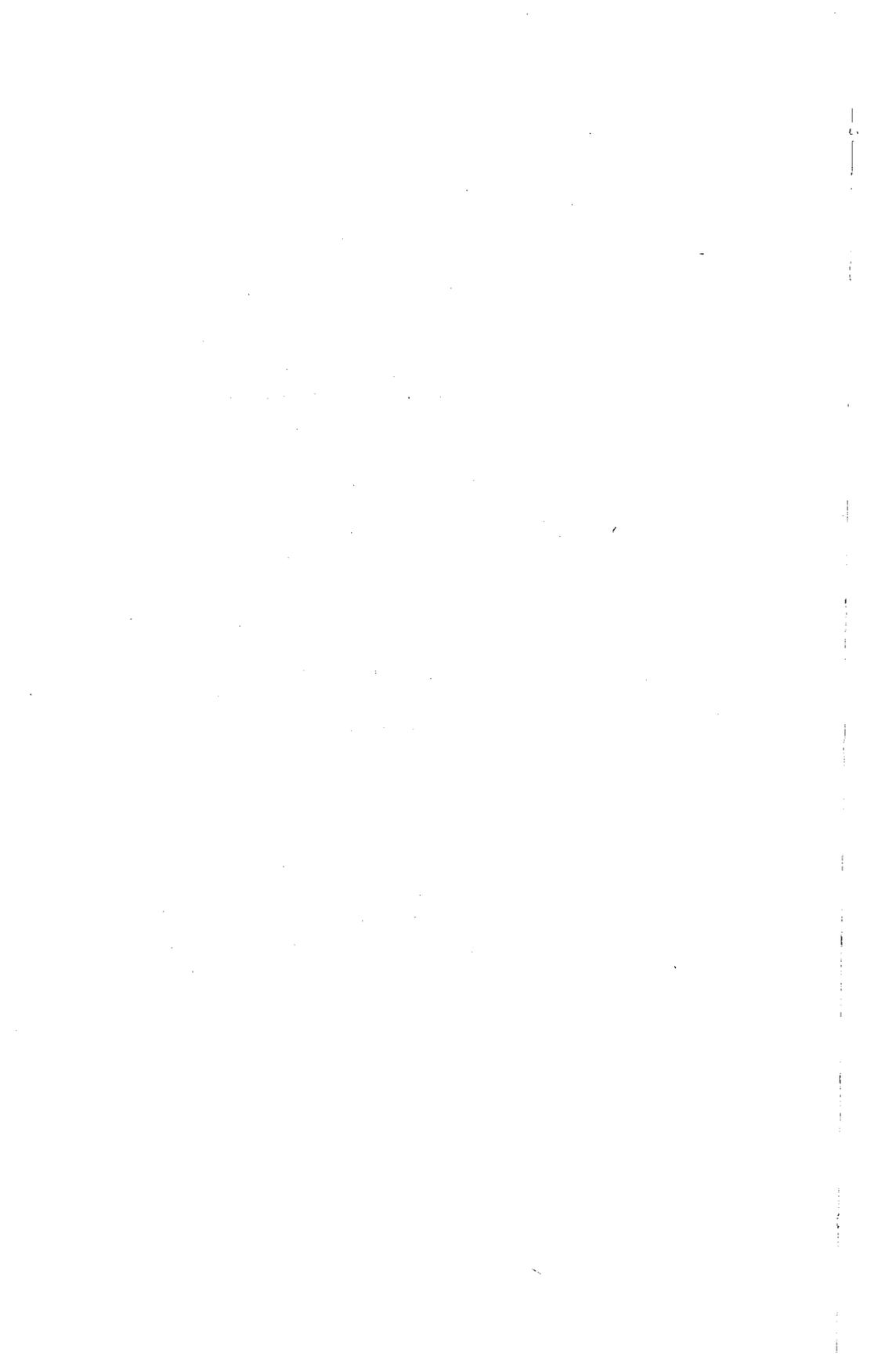
I.	El tratamiento de datos como una actividad económica lícita	113
II.	El derecho de propiedad en el tratamiento de datos de carácter personal ..	119
III.	El respeto a la vida privada en el tratamiento de datos	122

RÉGIMEN DE LOS BANCOS DE DATOS DE ORGANISMOS PÚBLICOS. UNA APROXIMACIÓN DEL DERECHO ADMINISTRATIVO A LA LEY SOBRE PROTECCIÓN DE LA VIDA PRIVADA
Ramiro Alfonso Mendoza Zúñiga

I.	Introducción	131
II.	¿Materia de ley?.....	134
III.	La Actividad Registral de la Administración y la publicidad de Registros	137
IV.	Actividad Registral y Principio de Legalidad.....	143
V.	Otros problemas disciplinares	149
VI.	Conclusiones	152

MODELOS COMPARADOS DE PROTECCIÓN DE LA INFORMACIÓN DIGITAL Y LA LEY CHILENA DE DATOS DE CARÁCTER PERSONAL
Francisco González Hoch

I.	Privacidad, intimidad e información digital	153
II.	Tensiones o conflictos en la regulación legal contemporánea de la información digital	159
III.	Alcance de la protección a la información digital en el derecho comparado	168
IV.	Principios y reglas en la regulación de la información comercial digital en el derecho comparado	171
V.	La nueva ley chilena de protección de datos de carácter personal (Ley N° 19.628) en la perspectiva del derecho comparado ..	174



PRÓLOGO

Los trabajos que constituyen el volumen en su mayor parte traen su origen en un Seminario sobre "Derecho a la Intimidad y Banco de Datos Personales", que fuera organizado por la Facultad de Derecho de la Universidad de los Andes, con motivo de la publicación de la ley chilena N° 19.628, sobre protección de datos personales, y cuya conferencia inaugural sobre el derecho fundamental a la intimidad fue ofrecida por quien suscribe estas líneas. Con gusto asumo ahora la labor de prologar el fruto de esa actividad con ocasión de la cual tuve la oportunidad de conocer y departir con los juristas chilenos.

La labor de edición, que con frecuencia se toma sus tiempos, ha permitido decantar aquellas primeras aproximaciones, y hoy se ofrecen en toda su sazón. El libro se abre con el trabajo de Felipe Vial Claro que en forma panorámica nos introduce en la nueva normativa chilena, similar en estos a otras como la LORTAD española de 1992. El ámbito de la aplicación de la ley chilena es circunscrito ya que según Vial sólo se aplicaría al "tratamiento organizado de datos personales", lo que excluiría el tratamiento de informaciones relevantes que esporádicamente pudieran efectuar terceros no dedicados empresarialmente a esa actividad.

El enfoque de la regulación chilena reside, por lo que se ve, en el respeto de los derechos de las personas, y fundamentalmente de la intimidad, de cara a las empresas o los servicios de la Administración que mantienen un registro o base de datos de carácter personal. En el artículo que sigue al de Vial, Hernán Corral

efectúa una enumeración de los diversos derechos o facultades que la ley consagra a los ciudadanos chilenos frente a los titulares de bancos de datos: de acceso a los datos del registro, de modificación de ellos, de "bloqueo" o suspensión de su vigencia, de cancelación, de copia, de aviso a terceros y de oposición. Como medio de tutela, la ley establece un procedimiento especial ante los tribunales civiles, que el autor denomina "amparo digital" y que es lo que internacionalmente se ha dado en llamar "habeas data". Hay también una mención del régimen especial de responsabilidad civil, para el que la introducción de un elemento normativo: la exigencia de que se trate de un procesamiento "indebido", hace concluir a Corral que la normativa no ha logrado zafarse del modelo subjetivo de responsabilidad.

Es evidente que una gran parte de la información que hoy día interesa es la de contenido económico o financiero. El estudio de Rony Jara pone al descubierto las ambigüedades que presenta el texto de la ley sobre este tipo de información, ya que si bien por una parte no es calificada de "dato sensible", para los que prevalece la denominada "autodeterminación informativa", mantienen una restricción de comunicación a terceros que los desmarca de los simples datos personales. El autor es partidario de interpretar esta tensión normativa haciendo primar el interés supraindividual de garantizar la transparencia crediticia: para "los datos comerciales no existe la facultad de autodeterminación y, por el contrario, si surge un conflicto debería prevalecer el interés supraindividual, traducido en la libertad de informar, porque allí no hay secreto legítimo". Se trata por cierto de un punto de equilibrio muy difícil de establecer y no extraña que haya visiones diversas. De hecho en este mismo libro, el trabajo de Renato Jijena desde su título se plantea como una aproximación "crítica" a la regulación de la ley 19.628,

por estimar que ella no ha significado un avance efectivo en el control del manejo de información relevante por parte de los agentes económicos. Se critica así que se otorgue plena libertad para el tratamiento de datos obtenidos de "fuentes accesibles al público", que, según el autor, de excepción deviene en regla general, con el agravante de que no se especifica qué debe entenderse por tales. Critica también que no se distinga entre información comercial positiva (contenido del activo patrimonial de las personas) e información comercial negativa (incumplimientos o moratorias), y estima inconstitucional que se permita el tratamiento no autorizado de la primera.

Con ello arribamos al tratamiento propiamente constitucional del derecho a la intimidad y la actividad de procesamiento de datos, que es materia de la intervención del destacado constitucionalista chileno Raúl Bertelsen. Para Bertelsen el tratamiento de datos personales debe ser comprendido dentro de las actividades económicas lícitas que se admiten en un sistema de economía de mercado y que, en Chile, encuentra respaldo en la propia Carta Fundamental cuando consagra el "derecho a desarrollar cualquiera actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, respetando las normas legales que regulen". De esta forma, piensa el constitucionalista que la ley 19.628 constituye, al menos en parte, el marco legal que regula, sin suprimirla o limitarla esencialmente, la actividad económica (lucrativa) de tratamiento de datos. Para el desarrollo de una actividad económica el reconocimiento de derechos de propiedad es indispensable, y según Bertelsen no debiera haber impedimentos para otorgar protección jurisdiccional a la propiedad que su titular tuviera de bancos de datos personales a condición de que éstos fueran "lícitamente obtenidos".

Pero no sólo las empresas, bancos y casas comerciales se interesan por la información personal de sus clientes, sino que también la Administración pública. La ley chilena contiene una regulación especial para los bancos de datos de organismos públicos, la que es analizada en el trabajo de Ramiro Mendoza. Como advierte Mendoza, en los tiempos que corren proliferan cada vez más los registros y archivos de organismos públicos, que pueden o no ser abiertos a todos los ciudadanos. Al incidir la información recogida en muchos de esos registros en la vida privada de las personas, derecho fundamental tutelado en la Constitución chilena, sólo la ley podría atribuir la potestad a la Administración de crear un registro y sólo para aquella información que sea relevante según la naturaleza del órgano del Estado o necesaria para el cumplimiento de los fines o funciones de éste. Se trata de la aplicación de lo que el autor designa como "criterio de especialidad".

Levantando la mirada para apreciar el contexto en el que surge la legislación chilena de protección de datos, cierra el volumen el estudio de Francisco González que es una síntesis de las direcciones y tendencias que se aprecian en el Derecho comparado, en especial en el Derecho estadounidense (cuna del "right to privacy") y el Derecho europeo (para el que el Tribunal Constitucional Federal alemán formulara el derecho a la autodeterminación informativa). Las diferencias entre estos dos sistemas parecen provenir, según explica González, de una diferente aproximación: mientras para los Estados Unidos el tratamiento de datos sería en general permitido y sólo se excluiría lo expresamente vedado, en el contexto europeo, cuyo caso paradigmático lo constituiría la legislación alemana, se partiría de la premisa opuesta, a saber, que el procesamiento de datos personales está prohibido salvo que haya autori-

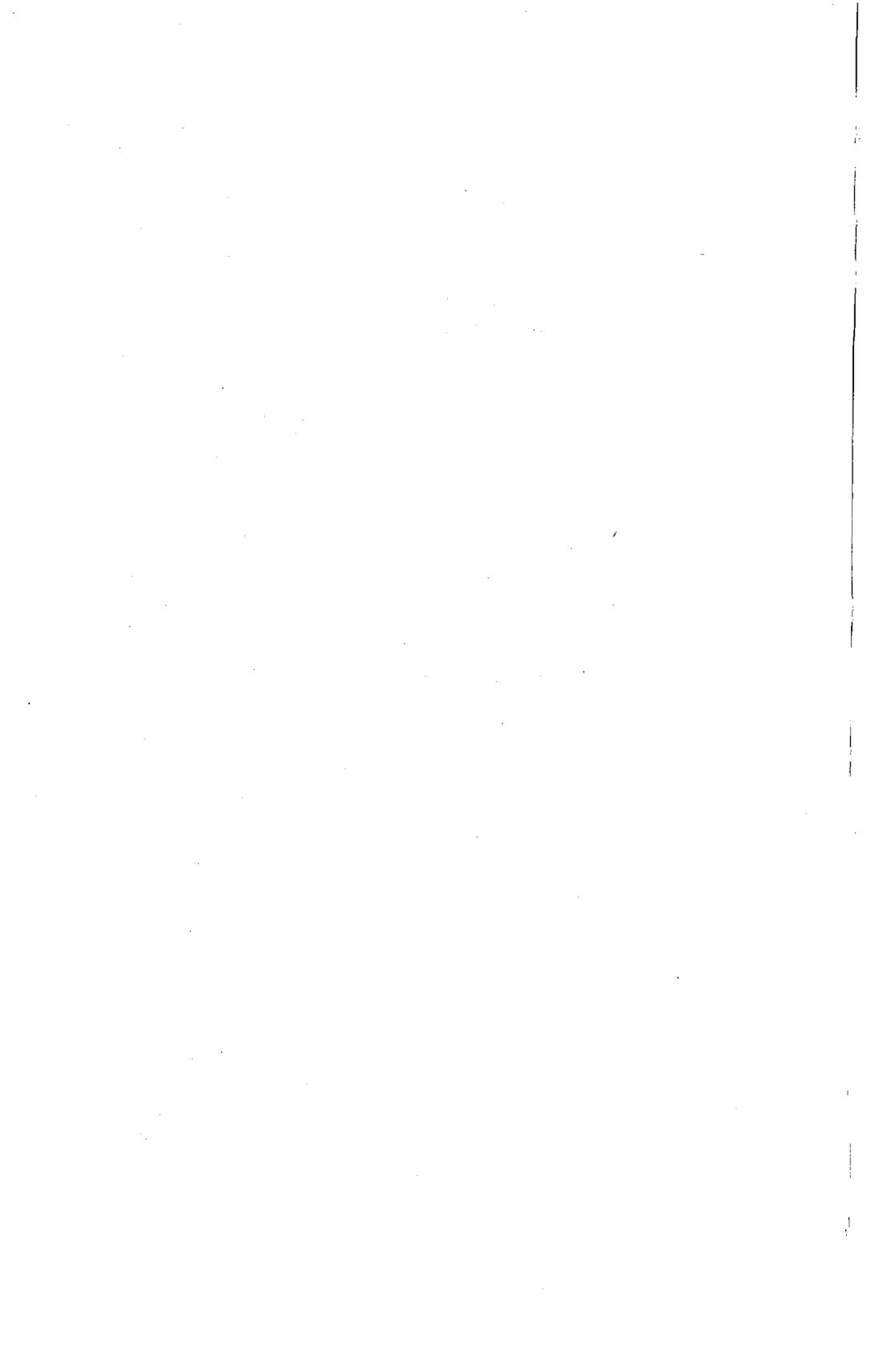
zación expresa del poder público. Al comentar la ley chilena, se advierte que el autor se siente más inclinado a aceptar como más razonable esta última actitud, puesto que califica de defectos de la ley chilena la inexistencia de una autoridad pública reguladora y la falta de un registro general de bases de datos que incluya a las bases privadas.

Con lo que he escrito hasta aquí, queda ofrecido al lector de esta obra un breve panorama de los temas que toca el libro que prologo y de las líneas maestras de lo que se dice sobre ellas. Me queda ahora dar un juicio sobre todo, juicio que no sólo creo que debe ser favorable, sino altamente elogioso, tanto por la pulcritud y acierto con que son tratados los extremos que se estudian, como porque no se echa en falta ninguno de los que corresponde examinar, y porque, finalmente, el estudio de todos ellos se hace avalado por la más completa documentación correspondiente al que sea, tocando los puntos en cada caso procedentes, sin digresiones inoportunas, ni entrar en cuestiones marginales, con visión aguda de lo que se examina y conclusiones fundamentadas, expuestas claramente y, yo diría, que acertadas siempre.

Por eso, desde aquí quiero proclamar mis mayores parabienes al libro, a sus autores y a la Colección Cuadernos de Extensión Jurídica, por publicarlo.

Madrid, diciembre de 2001

MANUEL ALBALADEJO GARCÍA
*Catedrático de Derecho Civil
Presidente de la Real Academia
de Jurisprudencia y
Legislación de España*



PRESENTACIÓN DEL EDITOR

Los trabajos recopilados en el presente volumen son fruto del esfuerzo académico de sus autores en relación con el Seminario "Derecho a la Intimidad y Bancos de Datos Personales" organizado por la Facultad de Derecho de la Universidad de los Andes en septiembre de 1999.

En esa ocasión y a sólo un mes de la publicación de la Ley 19.628 sobre Protección de Datos de Carácter Personal, los distintos expositores nacionales y extranjeros analizaron los desafíos que enfrenta el Derecho moderno, especialmente de cara al desarrollo de las bases de dato electrónicas, frente a la tarea de armonizar la protección de la vida privada con la autonomía empresarial y los intereses sociales involucrados en el tratamiento y difusión de ciertos datos. Dicha actividad académica fue realzada con una conferencia inaugural del tratadista español y maestro de civilistas don Manuel Albaladejo García.

Como en esa oportunidad, el presente volumen aporta distintos enfoques a las materias reguladas en la Ley desde las perspectivas de la dogmática civil, comercial, constitucional, administrativa y del Derecho comparado. De más está insistir en la importancia del aporte de los juristas a la hora de interpretar esta ley, cuando sus propias disposiciones ponen de manifiesto las variadas aristas y contrapuntos a considerar tras el principio de 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".

Es así como la estructura y organización general de la Ley es analizada con detención en el artículo del profesor Felipe Vial. A partir del ámbito de aplicación de la normativa —por cierto no limitada al tratamiento electrónico de datos— se tratan las principales definiciones, el marco regulatorio de los distintos bancos de datos, los principios que inspiran a dichas normas y las sanciones previstas para el caso de infracción.

Desde la perspectiva de las personas naturales titulares de la información —en principio las únicas amparadas por la norma—, el estudio del profesor Hernán Corral se centra en la naturaleza, contenido, límites y protección de los derechos subjetivos reconocidos por la nueva legislación. En esa línea se pueden distinguir los derechos de acceso —referido a la existencia y contenido del dato registrado—; de modificación de datos erróneos equívocos o incompletos; de bloqueo de datos proporcionados voluntariamente o que se usen en comunicaciones comerciales, y de cancelación de datos cuando su almacenamiento carezca de fundamento legal o se encuentren caducos.

En lo tocante al tratamiento de datos de carácter económico, financiero, bancario y comercial, el profesor Rony Jara analiza la normativa de la Ley 19.628 en referencia al Derecho comparado, teniendo como punto de partida las variables económicas y constitucionales envueltas en los intereses en juego. Las normas de la Ley revelan la permanente tensión entre el aseguramiento de los beneficios de una mayor disponibilidad de información y la necesidad de proteger la vida privada de las personas. Esta dinámica no ha sido resuelta adecuadamente por el legislador a juicio del profesor Jara, especialmente cuando la comunicación de antecedentes comerciales sin autorización del titular queda restringida a un listado de casos, abierto a ulteriores adiciones vía potestad reglamentaria.

Con el acento puesto en la tutela de la privacidad, la crítica del profesor Renato Jijena apunta a la inadecuada determinación de la esfera de datos privados merecedora de la protección legislativa. En particular, en este trabajo se hace notar la amplitud del concepto de datos accesibles al público, unida a la amplia autonomía que se reconoce a la actividad de tratamiento de los mismos sin necesidad de contar con la autorización del titular. Por otro lado, y volviendo al tema de los datos comerciales, el profesor Jijena enfatiza la necesidad de distinguir entre datos “positivos” y “negativos”, correspondiendo estos últimos básicamente a la información sobre incumplimientos, en que el interés social parece imponerse por sobre el interés en la privacidad, distinción de la que la Ley no se ocupa debidamente, en desmedro de la protección de la privacidad.

Desde la perspectiva netamente constitucional, el profesor Raúl Bertelsen analiza la actividad de los administradores de bases de datos a partir de la garantía al desarrollo de actividades económicas lícitas, y de las regulaciones legales —como la de la Ley que aquí interesa— que puedan serle aplicables en razón de la garantía a la vida privada de las personas. En cuanto a esta segunda garantía, el autor enfatiza la reserva legal en cuanto a su regulación o limitación, y propone sus dudas acerca de la constitucionalidad de las disposiciones que confieren potestad a las autoridades administrativas para legitimar la difusión de datos personales sin la autorización del titular. Por otro lado, los distintos grados de protección de la vida privada pueden ser apreciados en escala creciente, en función de la distinción entre datos accesibles al público, datos personales en general y datos sensibles.

El ámbito de reserva legal a la hora de regular garantías constitucionales es también una preocupación central en el artículo del profesor Ramiro Mendoza.

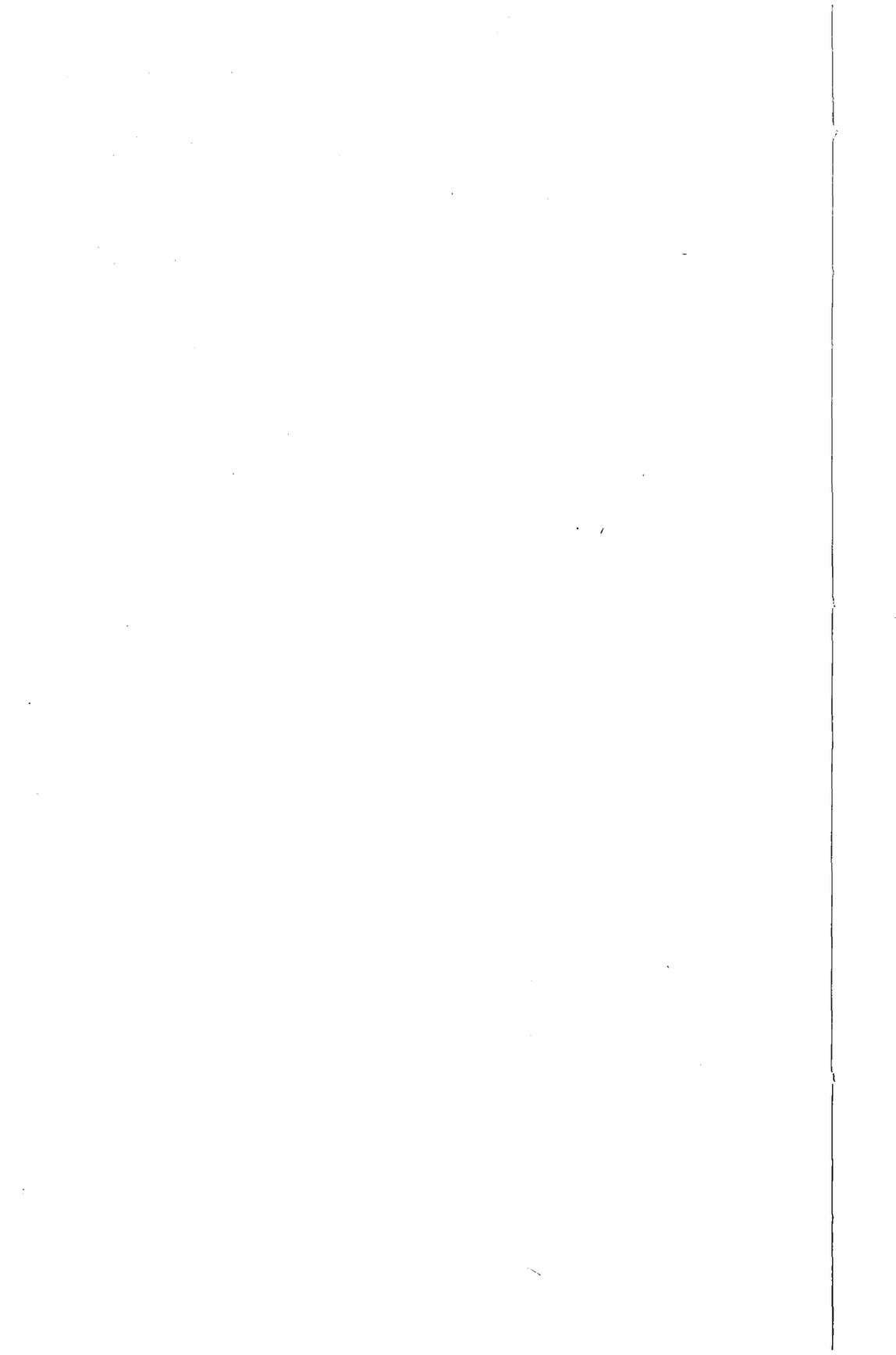
Sin embargo, en este caso el análisis se concentra en la creación y operación de bases de datos al interior de la administración pública. Al respecto, el autor observa con preocupación —desde el punto de vista de la protección de la vida privada— la opción seguida por el legislador en cuanto a reconocer la competencia para efectuar el tratamiento de datos cada vez que ello sea indispensable para el cumplimiento de las tareas del respectivo organismo público y dentro de su competencia general; lo anterior frente a la alternativa de exigir una habilitación legal específica. En todo caso, como lo precisa el autor, tal competencia general debe entenderse sin perjuicio de la norma que restringe el tratamiento de datos personales a los casos en que —ausente el consentimiento expreso del titular— la ley lo autorice.

Por último, los objetivos centrales de la nueva legislación son analizados sistemáticamente desde el punto de vista del Derecho comparado en el estudio del profesor Francisco González. En este caso la dinámica de la protección del interés público en la información, de la actividad empresarial de los operadores de bases de datos y de la protección a la vida privada, es estudiada a partir del desarrollo legislativo en Europa y los Estados Unidos, ocurrido a la par del vertiginoso desarrollo de la informática en las últimas décadas. Más allá del innegable valor del Derecho comparado en materia de interpretación de esta nueva legislación, cuya historia legislativa no oculta la referencia a las fuentes comparadas objeto del análisis, este estudio aporta nuevas y valiosas perspectivas para enjuiciar las regulaciones introducidas en Chile. Al respecto, es también interesante constatar las diferencias patentes entre la aproximación europea y norteamericana tanto en ésta como en otras materias. Sin embargo, parece al menos dudoso que la Ley chilena pueda proporcionar un nivel de

protección a la vida privada equiparable al de las fuentes comparadas invocadas durante la tramitación legislativa.

JORGE WAHL SILVA

15 de diciembre de 2001



**LA LEY N° 19.628 SOBRE
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
UNA VISIÓN GENERAL**

FELIPE VIAL CLARO
Profesor de Derecho Civil
Universidad de los Andes

I. ÁMBITO DE APLICACIÓN

1. LIMITADO ÁMBITO DE LA LEY

Tal como el proyecto fue definitivamente aprobado por el Poder Legislativo y contrariamente a lo que su título sugiere, la ley no regula orgánicamente todos los aspectos de la vida privada de las personas, entre los que podrían haber quedado comprendidas materias tales como la violación de domicilio, la violación de la correspondencia, la interceptación de las comunicaciones y, en general, la protección del honor, la imagen y la intimidad de las personas.

Por el contrario, la norma regula de una manera muy específica el tratamiento de los datos de carácter personal en registros o bancos de datos (art. 1°). La ley protege la vida privada de las personas naturales en cuanto ésta puede verse afectada por la recolección, registro, procesamiento, comunicación o utilización que se haga de cualquier forma, manual o automatizada, de sus datos personales, en registros o bancos de datos, por parte de personas u organismos públicos o privados.

2. TRATAMIENTO DE DATOS PERSONALES EN REGISTROS

O BANCOS DE DATOS

A la hora de establecer el ámbito de aplicación de la ley resulta crucial precisar lo que ésta entiende por tratamiento de datos personales (arts. 1º y 2º).

La letra o) del artículo segundo proporciona una amplísima definición de "tratamiento de datos". Ésta comprende básicamente toda operación o procedimiento técnico que permita recolectar, almacenar, procesar, comunicar o utilizar datos personales. La norma se refiere concretamente a la recolección, almacenamiento, grabación, organización, elaboración, selección, extracción, confrontación, interconexión, disociación, comunicación, cesión, transferencia, transmisión, cancelación o utilización en cualquier forma, largo listado de operaciones que revela el propósito del legislador de definir un concepto lo más amplio posible a este respecto. Es en todo caso indiferente que dicho tratamiento se efectúe por medio de procedimientos automatizados o no.

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

Es interesante también hacer notar que el tratamiento de datos personales objeto de regulación por la ley es aquel que se hace en registros o bancos de datos, definidos como conjuntos organizados de datos personales, manuales o automatizados, que permiten relacionar los datos entre sí y realizar todo tipo de tratamiento de los mismos (art. 2º, letra m).

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

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

3. CONCLUSIONES

En definitiva, puede concluirse que es objeto de la nueva ley:

- i) El tratamiento organizado de datos personales: esto es, el tratamiento de datos personales en registros o bancos de datos personales, y no el tratamiento de datos personales que pueda ocasionalmente efectuarse por un sujeto.
- ii) El tratamiento manual o automatizado de dichos datos: no es del todo relevante el que el tratamiento de datos personales sea efectuado manual o automatizadamente, sin perjuicio de que la automatización haya sido un factor determinante para la dictación de una ley en este sentido.
- iii) El tratamiento de datos efectuado por personas u organismos públicos o privados: no es en principio relevante la distinción entre personas u organismos públicos o privados.

El tratamiento de datos que se efectúe en ejercicio de la libertad de opinión y de informar no queda sujeto a esta ley.

II. MARCO REGULATORIO DEL TRATAMIENTO DE DATOS PERSONALES

1. CONVENIENCIA SOCIAL DE LOS REGISTROS O BANCOS DE DATOS

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. Es el caso de los bancos de datos con información económica, financiera, bancaria y comercial, que sirven de sustento al sistema crediticio (art. 4°). Así también, la norma se refiere a los bancos de datos con información de salud, que existen en apoyo del sistema de seguros de salud y del sistema previsional (art. 10). Implícitamente se comprenden también los bancos de datos con información de contribuyentes, en sustento del sistema impositivo del Estado (arts. 15 y 20). Igualmente, es el caso de los bancos de datos con información procesal y penal (art. 21), en apoyo del sistema procesal, penal y otras muchas instituciones y actividades en que como requisito se exige una conducta intachable de las personas. Un rol de evidente importancia corresponde a los

bancos de datos con información civil, como base del sistema de identificación y determinación del estado civil de las personas (art. 20). Asimismo, la existencia de bancos de datos con información sobre las personas, sus ideologías, actividades, opiniones, etc., se justifica como relevante para la seguridad nacional (art. 15).

2. PROTECCIÓN DE LA VIDA PRIVADA

Como contrapartida al reconocimiento de la conveniencia social de los registros y bancos de datos, la ley busca amparar a las personas que pueden ver afectada su vida privada y, particularmente, su honor, imagen e intimidad, por el tratamiento organizado de sus datos personales.

En vista a armonizar los intereses comprometidos, en primer lugar, junto con legitimar el tratamiento organizado de datos personales sólo en ciertas y determinadas circunstancias, la ley regula el desarrollo de esta actividad por parte de personas y organismos públicos y privados.

En segundo término, la norma en estudio reconoce y regula determinados derechos de las personas, concretamente del titular de los datos, con miras a evitar que el tratamiento organizado de sus datos personales pueda atentar en contra de su vida privada y, como se ha dicho, de su honor, imagen e intimidad.

III. PRINCIPIOS RECTORES DEL DESARROLLO DE LA ACTIVIDAD DE TRATAMIENTO ORGANIZADO DE DATOS PERSONALES

1. PRINCIPIOS MATRICES

Toda persona puede efectuar el tratamiento de datos personales sujeto a ciertos principios generales (art. 1º, inciso 2º).

Por un lado, dicho tratamiento debe efectuarse de conformidad a la ley en estudio y, muy específicamente, sólo para las "finalidades permitidas por el ordenamiento jurídico".

Por otra parte, el tratamiento de datos debe llevarse a cabo respetando el pleno ejercicio de los derechos fundamentales de los titulares de datos y de las facultades que la misma ley en estudio les reconoce.

2. DEBER DE CUMPLIR LA LEY Y FINALIDADES PERMITIDAS EN EL ORDENAMIENTO JURÍDICO

Sin perjuicio de la amplitud con la que aparece enunciado el principio matriz del libre tratamiento de datos personales, la ley a continuación precisa que dicho tratamiento sólo puede efectuarse cuando lo autoriza el titular de los datos o la ley (art. 4°).

En efecto, una primera posibilidad es que el propio titular de los datos personales autorice el tratamiento de los mismos, caso en el cual la autorización se sujeta a las siguientes reglas:

a) La autorización debe ser escrita e informada: la información que debe proporcionarse al titular de los datos debe cubrir tanto la finalidad dentro de la cual se enmarcará el tratamiento de datos como su posible comunicación al público, lo que dice relación con el grado de divulgación de sus datos personales que el titular está dispuesto a tolerar.

b) La autorización puede ser revocada: la revocación debe hacerse igualmente por escrito y en ningún caso opera con efecto retroactivo (art. 4°).

Una segunda posibilidad es que el tratamiento de los datos personales sea autorizado por la ley, sea que la autorización esté contenida en una ley especial (art. 4°) o que genéricamente se encuentre establecida en la Ley N° 19.628. En forma algo inorgánica esta ley, en definitiva, autoriza genéricamente el tratamiento organizado de datos personales en cuatro casos, a saber:

a) En el evento de tratamiento de datos personales provenientes de fuentes accesibles al público (no reservado a solicitantes), y siempre que se trate alternativamente:

- i) de datos personales de carácter económico, financiero, bancario o comercial;
- ii) de datos personales que se contengan en listados relativos a categorías de personas, que se limiten a indicar antecedentes tales como: pertenencia a un grupo, profesión o actividad, títulos educativos, dirección, fecha de nacimiento, o

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

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

- i) de datos personales para uso de la misma persona privada, sus asociados o afiliados, y
- ii) se traten sólo con fines estadísticos de tarificación u otros de beneficio general de los mismos (art. 4° inc. final). Quedará entonces por determinarse la amplitud de esos otros fines, por ejemplo en lo relativo a investigación histórica o científica.

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

d) Cuando el tratamiento de datos personales se efectúe para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (art. 10). Se trata aquí de un caso especialísimo, en el que la ley autoriza incluso el tratamiento de datos sensibles, que se refieren a 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, los estados de salud físicos o psíquicos y su vida sexual. De acuerdo a la letra g) del artículo segundo, son también datos sensibles, aunque en otro orden de materias, las ideologías, opiniones políticas y creencias o convicciones religiosas.

3. DEBER DE RESPETO A LOS DERECHOS DEL TITULAR DE LOS DATOS

La ley concede la condición de titular de los derechos que en ella se reconocen al titular de los datos, únicamente a las personas naturales y no a las personas jurídicas, cuestión que tiene su justificación en la arraigada convicción de que el honor, la imagen y la intimidad, que esta ley tiene por objeto proteger, son atributos morales que corresponde por su naturaleza sólo a las personas naturales.

Sin perjuicio de los derechos fundamentales que reconoce la Constitución Política del Estado en relación a la vida privada de los individuos, la lectura y análisis de la ley conduce a reconocer en favor del titular de datos los siguientes derechos:

3.1. Autorización previa

La ley de alguna manera reconoce a las personas naturales el derecho a que sus datos no sean incluidos en un registro o banco de datos personales sin previa autorización del mismo titular o de la ley.

El derecho antes mencionado está asegurado con el reconocimiento de las siguientes facultades:

a) La facultad de acceder al registro o banco de datos personales: en efecto, la ley reconoce la facultad de exigir gratuitamente, de quien se dedique al tratamiento público o privado de datos personales, información sobre los datos personales contenidos en el respectivo registro o banco de datos, su procedencia, destinatarios, la finalidad del almacenamiento y la individualización de las personas a quienes sus datos son transmitidos regularmente (art. 12 inc. 1°).

b) La facultad de exigir la eliminación de datos personales: la ley también reconoce la facultad de exigir gratuitamente la eliminación de datos personales de un registro o base de datos, entre otras razones, por la revocación de la autorización o por falta de fundamento legal (art. 12 inc. 3°).

3.2. Sujeción del tratamiento a una finalidad

En este sentido, la ley reconocería a las personas naturales el derecho a que sus datos personales no sean objeto de tratamiento, sino únicamente para aquellas finalidades expresamente autorizadas por el propio titular o la ley. Este derecho se asegura con el reconocimiento de las siguientes facultades:

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

b) Facultad de acceder al registro o banco de datos personales, en los términos ya comentados precedentemente (letra a) apartado 3.1.).

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

- i) del carácter obligatorio o facultativo de las respuestas, y
- ii) el propósito o finalidad para el cual se está solicitando la información (art. 3°).

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

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

f) Facultad de eliminar datos personales, en los términos ya comentados precedentemente (letra b) apartado 3.1.).

3.3. Veracidad de la información

Sobre el particular, las personas naturales tienen derecho a que la información a su respecto contenidas en los registros o bases de datos personales sea exacta, actualizada y responda con veracidad a situación real del titular de los datos (art. 9°). Junto con reconocer este derecho, la ley contempla una serie de disposiciones tendientes a hacerlo efectivo:

a) Facultad de acceder al registro o banco de datos personales, comentada en los dos numerales precedentes.

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

- 1° Facultad de eliminar datos: de acuerdo al artículo 12, la caducidad de la información autoriza a exigir la eliminación de los datos. En este caso debe procederse en general a la destrucción de los datos y, además, a dar aviso de la eliminación de un modo particular a quienes se hubiere comunicado dicha información o, de un modo general, si lo anterior no es posible, mediante un aviso que pueda ser de conocimiento general de los usuarios del respectivo banco de datos.
- 2° Facultad de modificar datos: la misma norma mencionada autoriza a exigir la modificación de datos erróneos, inexactos, equívocos o incompletos, caso en el cual debe procederse a cambiar el contenido de los datos almacenados y, además, a dar aviso de la modificación, en los mismos términos comentados en el párrafo anterior.
- 3° Facultad de bloquear datos: si no corresponde la eliminación, puede solicitarse el bloqueo cuando la exactitud de los datos no puede ser establecida o si su vigencia es dudosa, caso en el cual debe procederse a la suspensión de toda forma de tratamiento (arts. 12 y 6°).

Más aún y conforme lo establece el artículo sexto, el responsable del banco de datos debe proceder a la eliminación, modificación o bloqueo de los datos, según corresponda, sin necesidad de requerimiento del titular.

Sin embargo, el derecho a exigir la eliminación, modificación o bloqueo de datos reconoce algunas excepciones, las que tienen lugar cuando el ejercicio de dichas facultades impide o entorpece el debido cumplimiento de funciones fiscalizadoras del organismo público requerido (como podría ser el caso del SII), afecta la reserva o secreto establecidos en leyes y reglamentos, afecta la seguridad de la nación o el interés nacional, o también cuando tales facultades no fueren reconocidas al titular en la ley que haya ordenado el almacenamiento de los datos (art. 15).

En todo caso, la facultad de eliminar, modificar o bloquear datos no puede ser limitada bajo respecto alguno por actos o convenciones de partes (art. 13).

c) Exactitud, actualización y veracidad de información sobre obligaciones: especial relevancia tiene el derecho a la veracidad de la información cuando ella se refiere a las obligaciones de una persona, razón por la cual la ley establece a este respecto que sólo puede comunicarse información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en ciertos y determinados títulos, a saber, letras de cambio y pagarés protestados; cheques protestados por falta de fondos, cuenta corriente cerrada u otra causa; mutuos hipotecarios, préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorro y crédito, organismos públicos y empresas del Estado sometidas a la legislación común, y administradoras de crédito otorgados para compras en casas comerciales, y obligaciones de dinero que determine por Decreto Supremo el Presidente de la República, siempre que estén sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los que conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento.

Por otra parte, la posibilidad de dar información a este respecto se limita en el tiempo a no más de 7 años del vencimiento de la respectiva obligación y a no más de 3 años de su pago o extinción por otra causa. Lo anterior, entre otras razones, con el objeto de velar por la exactitud y actualización de la información y que ella describa fielmente la situación real de la persona (arts. 17 y 19).

d) Exactitud, actualización y veracidad de información procesal y penal: especial relevancia tiene el derecho a la veracidad, también, cuando se trata de información personal de carácter procesal o penal, motivo por el cual la ley establece que los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias no podrán comunicarlas una vez prescrita la acción penal o administrativa, o una vez cumplida o prescrita la sanción o pena (art. 21). Nuevamente, la ley revela una preocupación por velar por la exactitud y actualización de la información y que ella describa fielmente la situación real de la persona.

3.4. Reserva y custodia de datos personales

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

Además, la ley obliga al responsable de la base de datos personales a cuidar dichos datos con la debida diligencia y lo hace responsable de los daños que pueda provocar al titular. La disposición en este sentido debe entenderse como la imposición de un deber de custodia, tendiente a evitar que los datos personales sean comunicados a personas no autorizadas o que las comunicaciones sean interceptadas por personas no autorizadas (art. 11).

3.5. Especialidad del tratamiento de datos sensibles

Las personas naturales tienen derecho a que sus datos sensibles no sean objeto de tratamiento, sino en virtud de autorización especial al efecto dada por el titular o la ley.

La simple autorización para efectuar el tratamiento de datos personales, según se desprende de lo dispuesto en el artículo 10, no es suficiente para legitimar el tratamiento de datos sensibles.

4. RECAPITULACIÓN

Las normas comentadas anteriormente y otra serie de disposiciones de la ley permiten distinguir los principios rectores a que en definitiva está sometido el tratamiento organizado de datos personales, a saber:

a) No puede efectuarse el tratamiento organizado de datos personales sin previa autorización del titular o de la ley (especialmente en el caso de datos sensibles).

b) El tratamiento organizado de datos personales sólo puede efectuarse con una finalidad determinada, explícita y legítima.

c) El tratamiento organizado de datos personales debe respetar el pleno ejercicio de los derechos fundamentales y legales del titular de los datos y, muy concretamente, la veracidad de la infor-

mación y la reserva y custodia de la información, para que ella no sea comunicada o interceptada por personas no autorizadas por el titular o la ley.

d) El tratamiento de datos personales está entregado a la responsabilidad del sujeto, sea persona u organismo público o privado, a quien competen las decisiones relacionadas con el tratamiento de los datos personales.

Es importante resaltar que la ley no contempla organismos administrativos a cargo del control de esta actividad y el principio, en definitiva, es que cualquier persona puede efectuar el tratamiento organizado de datos en la forma que dispone la ley, sin necesidad de registro previo. La única norma que hace excepción a este principio es aquella que obliga a los organismos públicos a comunicar al Servicio de Registro Civil e Identificación, cuando corresponda, la creación de un registro o banco de datos, los fundamentos jurídicos del mismo, su finalidad, tipo de datos almacenados y descripción del universo de personas que comprende. Al Servicio de Registro Civil e Identificación la ley encomienda llevar un registro de los bancos de datos a cargo de organismos públicos (art. 22).

IV. INFRACCIONES Y SANCIONES

1. DISTINTOS ÓRDENES DE INFRACCIONES Y SANCIONES

La ley contempla varios órdenes de infracciones y sanciones según sea el caso, las que pueden sintetizarse como sigue:

1.1. Infracción al deber de pronunciarse sobre la solicitud de entrega de información, modificación, eliminación, o bloqueo de datos: en estos casos, la persona afectada puede reclamar mediante un recurso especial de amparo, a través del cual puede obtenerse precisamente la información, modificación, eliminación o bloqueo de datos personales requerida y, además, la imposición de multas o suspensión del cargo a los responsables (art. 16).

1.2. Infracción a las normas sobre utilización de datos personales, relativos a obligaciones de carácter económico, financiero, bancario o comercial: en estos supuestos la persona afectada puede

reclamar, también mediante recurso especial de amparo, a través del cual puede obtenerse el cumplimiento de las obligaciones infringidas y, además, la imposición de multas o suspensión del cargo a los responsables (art. 19).

1.3. Otras infracciones: fuera de los casos tratados en los números precedentes, la persona afectada puede reclamar a través de demanda en juicio sumario especial, en el que se aprecia la prueba en conciencia y el juez deberá tomar todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece (art. 23).

2. RESPONSABILIDAD CIVIL

La ley dispone que, sin perjuicio de lo ordenado por el juez en su caso, la persona u organismo a cargo del registro o banco de datos deberá indemnizar el daño patrimonial y moral que causare el tratamiento indebido de los datos (art. 23).

Cabe entender que la responsabilidad civil impuesta sobre el responsable del registro o banco de datos es de naturaleza extracontractual y, por lo tanto, deben cumplirse al respecto los requisitos exigidos por la ley al efecto (art. 23).

En cuanto al autor, es claro puede tratarse de una persona natural o jurídica, pública o privada. A su vez, el hecho ilícito estará constituido por el tratamiento indebido de datos personales, lo cual supone un tratamiento con infracción de ley o que no respeta los derechos fundamentales o legales del titular de los datos (art. 23). En lo que atañe a la causalidad entre el hecho ilícito y el daño, la ley no aporta reglas especiales.

Respecto de 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 base de datos personales. Así, dicho sujeto se encuentra obligado a contar con la autorización del titular o de la ley para el tratamiento de los datos; a sujetar dicho tratamiento a la finalidad del respectivo registro; a cuidar la veracidad de la información, proporcionando la información que se le solicite respecto del mismo, modificando, eliminando y bloqueando los datos personales cuando ello proceda, y a cuidar los datos almacenados con la debida diligencia.

De esta manera, el sujeto responsable del registro o base de datos personales debe responder de las obligaciones apuntadas en

el párrafo precedente y de las demás que específicamente señala la ley al regular estas materias, responsabilidad o deber de cuidado que, de acuerdo al derecho común, se extiende hasta la culpa leve.

En lo concerniente a los daños, se responde de daño material y moral. Tratándose del daño material y concretamente del daño emergente y lucro cesante, cabe entender que se aplican las reglas generales, de acuerdo a las cuales el daño debe ser debidamente acreditado. A su vez, al daño moral se aplicaría la regla contenida en el artículo 23 de la ley, de acuerdo a la cual la evaluación del daño la hace el juez prudencialmente, considerando las circunstancias del caso y la gravedad de los hechos (art. 23).

Desde el punto de vista de la acción civil, ésta puede interponerse conjunta o separadamente con la reclamación destinada a establecer la infracción, esto es, conjunta o separadamente con la acción de amparo del artículo 16, la del artículo 19, o la demanda en juicio sumario en el caso de otras infracciones. Es motivo de reflexión el que junto con una acción de amparo se autorice discutir sobre la existencia del derecho a una indemnización e incluso sobre la especie y monto de los perjuicios.

En todo caso, la ley admite litigar sobre el derecho a la indemnización y separadamente sobre la especie y monto de los perjuicios (173 CPC). Si se sigue este procedimiento separado cabría entender que la acción de indemnización de perjuicios se sometería a las reglas del juicio sumario especial antes aludido (art. 23).

3. RESPONSABILIDAD PENAL

La ley no contempla sanciones penales, sin perjuicio de las penas que puedan establecer las leyes en casos específicos.

V. VIGENCIA

Habiendo transcurrido los plazos de vacancia legal, la ley se encuentra plenamente vigente a la fecha. Sin perjuicio de ello, es conveniente comentar algunas de sus normas transitorias, relativas a los efectos de la ley desde la fecha de su vigencia.

En efecto, según el inciso segundo del artículo primero transitorio, los actuales registros o bancos de datos personales de organismos públicos deberán ajustarse a las disposiciones de la nueva ley desde la fecha de su entrada en vigencia.

Por otro lado, de acuerdo al artículo segundo transitorio, los titulares de los datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de la ley tendrán los derechos que ésta les confiere.

Por último, de conformidad al artículo tercero transitorio, las normas que regulan el Boletín de Informaciones Comerciales creado por el D.S. 950 de 1928 seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de la nueva ley.

**DE LOS DERECHOS DE LAS PERSONAS
SOBRE LOS RESPONSABLES DE BANCOS
DE DATOS: EL *HÁBEAS DATA* CHILENO**

HERNÁN CORRAL TALCIANI
Profesor de Derecho Civil
Universidad de los Andes

I. INTRODUCCIÓN

1. ÁMBITO DE APLICACIÓN DE LA LEY N° 19.628
Y NOCIONES BÁSICAS

La ley regula la protección de datos de carácter personal, entendidos como cualquier información concerniente a una persona natural (art. 2°, letra f), respecto del tratamiento en registros o bancos de datos, por parte de personas u organismos públicos o privados.

Cabe recordar también que se utiliza un concepto amplio de tratamiento que incluye la recolección, almacenamiento, procesamiento, comunicación y toda forma de utilización de datos personales, sea de carácter manual o automatizado. Por registros o bancos de datos se entiende a los conjuntos organizados de datos personales, manuales o automatizados, que permiten relacionar los datos entre sí y realizar todo tipo de tratamiento de los mismos (art. 2°, letra m).

En general, sólo se autoriza el tratamiento de datos por dos formas, a saber, con el consentimiento específico del titular, en todos los casos en que se trate de datos sensibles, o con autorización legal, la que cubre el tratamiento de datos de fuentes accesibles al público (no reservados a los solicitantes). En cualquier caso, la utilización de los datos debe hacerse sólo para finalidades permitidas por el ordenamiento jurídico.

Sin perjuicio de lo anterior, existen normas especiales para el tratamiento de datos personales relacionados con beneficios de salud, para el que efectúan personas jurídicas privadas sobre sus asociados o afiliados (art. 4°), para el que puedan efectuar organismos públicos respecto de materias de su competencia, y para el tratamiento de datos personales relativos a información económica, bancaria o comercial.

2. DISTINCIÓN ENTRE DEBER GENERAL Y DERECHO SUBJETIVO

Para circunscribir debidamente el ámbito de este trabajo, hemos de recordar la distinción entre deberes generales y derechos subjetivos. Un deber general puede establecerse por el legislador sin necesidad de instaurar un derecho subjetivo correlativo con un titular identificable. Son obligaciones en un sentido público y no civil del término. La ley 19.628, de 1999, contiene numerosas enunciaciones de obligaciones o deberes en este sentido. Así, por ejemplo, la obligación de efectuar tratamiento de datos sólo cuando exista autorización expresa del titular o de la ley (art. 4°.1), la de resguardar los derechos de los titulares en la transmisión de datos (art. 5°), las de eliminar, modificar o bloquear datos sin necesidad de requerimiento (art. 6°), las de guardar reserva de las personas que trabajan en el tratamiento de información personal (art. 7°), la de no procesar datos sensibles salvo casos de excepción (art. 10).

En todos esos casos estamos frente a deberes que se imponen a los responsables de bancos de datos, esto es, a las personas naturales o jurídicas privadas u organismos públicos, a quienes competen las decisiones relacionadas con el tratamiento de datos de carácter personal (art. 2°, letra n), y cuya infracción podrá generar sanciones de carácter infraccional o disciplinario y también responsabilidad civil por los daños y perjuicios producidos. No estamos sin embargo en el ámbito de los derechos subjetivos.

El derecho subjetivo es la facultad moral de exigir que otra persona desarrolle un cierto comportamiento (dé, haga o no haga algo determinado). De esta manera, el sujeto pasivo resulta obligado, pero no tanto por la disposición de la ley, sino más bien por el reconocimiento que ella hace de un derecho perteneciente a otra persona. Es el derecho el que causa el deber u obligación.

La distinción es importante, pues mientras los deberes generales sólo son exigibles en los términos comprendidos en su descripción, los derechos permiten al titular exigir al obligado que desarrolle las

conductas necesarias para satisfacer el interés jurídicamente protegido por aquél.

Este trabajo se dirige por tanto a identificar y describir los derechos propiamente tales que la ley N° 19.628 reconoce o concede a los particulares frente al tratamiento de datos.

3. LA LEY N° 19.628 RECONOCE DERECHOS SUBJETIVOS

Pensamos que es indudable que la ley N° 19.628 no sólo prescribe deberes u obligaciones de carácter genérico, sino que establece claros derechos subjetivos. Es así como el título II de la ley, que se compone de los artículos 12 a 16, se denomina "De los derechos de los titulares de datos".

En realidad, sólo los artículos 12 a 15 contienen una regulación de los derechos de los titulares, mientras el artículo 16 se dirige a reglamentar la acción típica mediante la cual se busca asegurarles una tutela judicial efectiva.

La terminología de la ley, unida a la caracterización que ella hace de las facultades otorgadas a los particulares, o titulares de datos, hacen inexcusable la conclusión de que estamos frente a derechos subjetivos, esto es, a facultades morales que permiten a su titular exigir de otra persona una determinada conducta.

4. LOS TITULARES DE DATOS COMO SUJETOS DE DERECHOS

La ley ha concedido estos derechos a los "titulares de datos". Según la terminología fijada en el artículo segundo, titular de los datos es "la persona natural a la que se refieren los datos de carácter personal" (art. 2°, letra ñ). En otros términos, es lo que los autores españoles suelen denominar "persona concernida".

Debe notarse que se excluyen como sujetos de derechos a las personas jurídicas. La razón debe buscarse en la naturaleza de la información de que estamos hablando. En rigor, sólo sobre las personas naturales puede existir información de carácter personal. Esto aparece reafirmado en el artículo 2°, letra f, que define datos de carácter personal.

Hay que tener presente que los legisladores optaron por identificar a los sujetos de derechos como "titulares de los datos", modificando así el proyecto que fuera aprobado por la Cámara de Diputados que confería la titularidad de los datos a los administradores de bancos de datos. De esta forma, la ley reconoce que

existe un nexo entre la persona y el dato o información que concierne a ella.

¿Cuál es la naturaleza de este nexo? Parece que debe descartarse que estemos aquí frente a una propiedad, ya que el dato como tal, con independencia del soporte físico, electrónico o informático en el que se encuentre recogido, no es ni una cosa corporal ni una cosa incorporeal (derecho real o personal) ni una cosa intelectual (como una obra literaria o una marca o invención). El dato es un conocimiento adquirido por un tercero sobre una persona en cuanto representado funcionalmente para ser comunicable a un número indeterminado de usuarios. La persona tiene un cierto poder de control, entonces, no sobre el dato en sí, que es incorpóreo, sino sobre los medios empleados para su representación y comunicación.

De esta forma, la expresión "titulares de datos" resulta poco feliz desde un punto de vista dogmático, aunque puede ser útil para fines de claridad.

5. PLAN DEL TRABAJO

Aclarados los conceptos de derechos subjetivos y de sujetos de estos derechos en la normativa en estudio, nos abocaremos en primer lugar a analizar los derechos que aparecen legalmente recogidos en la ley (II); en segundo término haremos referencia a la forma de ejercicio de dichos derechos (III), así como a las excepciones que se contemplan respecto de ellos (IV).

Pasaremos luego a exponer la acción cautelar que se ha conocido en doctrina como *habeas data* y que la ley regula en su artículo 16 (V), como también el recurso del particular para hacer efectiva la responsabilidad civil del responsable de banco de datos personales en caso de incumplimiento de los deberes que establece la ley (VI).

Terminaremos con algunas reflexiones conclusivas sobre la naturaleza única o múltiple de estos derechos y su relación con la protección de la vida privada y la acción constitucional de protección (VII).

II. DERECHOS LEGALMENTE RECONOCIDOS

Nos parece que los derechos que la ley concede son los de acceso; de modificación, de bloqueo y de cancelación de datos. A ellos deben agregarse dos que son variantes de los anteriores: el de

copia y el de aviso a terceros. Finalmente, existe un supuesto restringido de derecho de oposición al tratamiento de datos.

1. DERECHO DE INFORMACIÓN O ACCESO

El llamado derecho de acceso significa tener la posibilidad de conocer la existencia de un determinado registro o banco de datos y la información que posee sobre una determinada persona.

El derecho, según el artículo 12 de la ley, consiste en la "facultad de exigir... información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente" (art. 12 ley N° 19.628).

En consecuencia, el derecho puede ejercerse con varios objetivos, a saber:

- Para saber si un determinado banco de datos contiene información sobre el requirente;
- Para saber el contenido de la información que posee el banco sobre el requirente;
- Para conocer el origen de los datos;
- Para conocer el destinatario para el cual fueron recogidos;
- Para conocer el propósito u objeto de su almacenamiento, y
- Para conocer las personas u organismos a los cuales los datos son transmitidos, esto es, comunicados, de manera regular.

Entendemos que el requirente en el ejercicio de este derecho deberá indicar si necesita toda la información referida. Si nada dice, lo razonable es pensar que el derecho de acceso se satisface con la información sobre la existencia y contenido de datos sobre el requirente en un determinado banco.

2. DERECHO DE MODIFICACIÓN

La ley denomina derecho de modificación a la facultad que tiene un titular de datos para alterar un registro de un banco de datos.

La necesidad de modificar puede provenir de las siguientes causas:

- Existencia de un dato erróneo o inexacto (art. 12.2): aunque la ley diferencie los vocablos, nos parece que coinciden; lo erró-

neo es inexacto y viceversa. Por ejemplo, la persona se llama Pedro y no Juan, o es chilena y no brasileña.

- Existencia de un dato equívoco (art. 12.2): se trata de una información que puede interpretarse en maneras diversas por falta de claridad. Por ejemplo, si aparece como oficio de una persona la de "procurador".
- Existencia de un dato incompleto (art. 12.2): es una información que aunque exacta es parcial. Por ejemplo, si se contempla que una persona viajó al extranjero, pero no se registra su regreso al país.

En verdad, sólo tratándose de los datos erróneos o equívocos cabe hablar de derecho a la modificación. Cuando existen datos incompletos, no hay propiamente modificación, sino complementación o integración. No obstante, la ley habla en general de modificación también en el caso de los datos incompletos: "En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen" (art. 12.2).

3. DERECHO DE BLOQUEO

El derecho a bloquear los datos consiste en la facultad de exigir que se suspenda temporalmente el tratamiento de datos que estén almacenados, es decir, que se suspenda cualquier operación o conjunto de operaciones o procedimientos técnicos destinados a utilizar los datos en cualquier forma (art. 2º, letras b y o).

El bloqueo no procede de manera general para todos los titulares de datos, sino sólo en los casos precisos determinados por la ley. Éstos son: 1º) que se trate de datos que el titular haya proporcionado voluntariamente; 2º) que se trate de datos que se usen para comunicaciones comerciales. Respecto de este segundo caso, debe tenerse en cuenta que la ley exime de la necesidad de obtener autorización del interesado para registrar sus datos, entre otros supuestos, a los listados de datos "que sean necesarios para comunicaciones comerciales de respuesta directa" (art. 4º.5).

En los dos casos señalados, el titular puede exigir al respectivo banco de datos que su información deje de ser utilizada de un modo temporal (art. 12.4).

No indica la ley el plazo por el cual procede el bloqueo, pero debe entenderse que la duración es indefinida, es decir, hasta que

exista expresión de voluntad en contrario del requirente. Esta conclusión se impone si se observa, como veremos a continuación, que por las mismas causales el titular puede pedir, no ya el bloqueo temporal, sino la eliminación o cancelación definitiva de sus datos.

4. DERECHO DE CANCELACIÓN

La eliminación o cancelación de los datos es "la destrucción de los datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello" (art. 2º, letra h).

El derecho a exigir la eliminación o cancelación procede en diferentes supuestos, a saber:

- Si el almacenamiento carece de fundamento legal (art. 12.3); es decir, por regla general si no aparece autorizado ni por el titular ni por la ley N° 19.628 ni por otra disposición legal.
- Si los datos tienen el carácter de caducos (art. 12.3), esto es, si han perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consignan (art. 2º, letra d).
- Si los datos han sido proporcionados voluntariamente o se usan para comunicaciones comerciales (art. 12.4).

5. DERECHO DE COPIA

Cuando el titular ejerce el derecho de modificación o cancelación, la ley le reconoce además el derecho de obtener copia del registro alterado en la parte pertinente (art. 12.5). Mejor que copia, lo que la ley exige es que se otorgue al particular afectado la representación en soporte físico del dato sobre el que se ha producido la modificación, o del resto del asiento referido a él, del cual se ha eliminado un elemento sobre el que se pidió la cancelación.

La obtención de esta copia es gratuita para el solicitante. Pero para evitar abusos se establece que si, efectuada una primera modificación o cancelación y ejercido el derecho de copia respecto de ella, se ejerce nuevamente el derecho de modificación o cancelación, el particular deberá pagar la copia, salvo que haya transcurrido un plazo mínimo de seis meses entre la primera y la segunda petición. La ley dice que el plazo de seis meses se cuenta "desde la

precedente oportunidad en que se haya hecho uso de este derecho" (art. 12.5). Nos parece que el momento desde el cual se debe contar este plazo no es la fecha de la petición, sino aquella en la que el banco de datos otorgó la respectiva copia, ya que sólo en este momento puede decirse que el solicitante "usó" (ejerció) este derecho.

6. DERECHO DE AVISO A TERCEROS

La ley supone que los datos que son objeto del derecho de modificación o cancelación pueden haber sido comunicados por el banco de origen a otras personas determinadas o determinables. De allí que obligue al responsable del banco a avisarles a esas personas la operación efectuada "a la brevedad posible" (art. 12.6).

En caso de que no sea posible determinar las personas a las que se hubieren comunicado los datos, el responsable deberá poner "un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos" (art. 12.6). La norma es poco precisa, y en caso de discordia será materia a resolver por el juez.

7. DERECHOS DE OPOSICIÓN

Aunque en título aparte, la ley menciona otro derecho de los titulares de los datos, es el derecho de oposición, según el cual, "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión" (art. 3°.2).

III. CONDICIONES DE EJERCICIO DE LOS DERECHOS

1. LEGITIMACIÓN ACTIVA

La legitimación activa de estos derechos parece corresponder a las personas naturales que la ley llama titulares de datos.

No obstante, pensamos que el derecho de acceso o de información es más extensivo ya que corresponde, como el mismo texto del inciso primero del artículo 12 señala, a "toda persona". Esto es así por cuanto no es necesario demostrar, para hacer uso de este derecho, que existe un dato del cual se es titular. Justamente, el derecho consiste en la posibilidad de una persona de indagar sobre

la existencia de información suya registrada y tal gestión puede concluir positiva como negativamente. En este último evento, habrá hecho uso del derecho de información sin tener la cualidad de titular de datos.

Los derechos de modificación, bloqueo y cancelación, en cambio, corresponden a quienes efectivamente tengan un nexo con una información personal que les atinge.

No pueden ser ejercidos por terceros para la protección de otros beneficiarios. La ley en el artículo 12 habla de derechos sobre "datos relativos a su persona", es decir, a la persona natural interesada.

¿Procederá la representación voluntaria o legal en el ejercicio de estos derechos? ¿Podrán, por ejemplo, el padre o la madre que ejerce la patria potestad ejercer estos derechos en representación del menor? ¿O un mandatario en representación de su mandante? Aunque podría objetarse que estamos frente a derechos de la personalidad que no admiten representación, somos de la opinión de que deben en este caso aplicarse las reglas generales de la representación y del mandato. De hecho, en forma explícita la ley señala que para el tratamiento de datos personales se admite el mandato, el que se rige por las reglas generales (art. 8º.1).

Únicamente respecto del derecho de copia, la ley exige ejercicio personal: "El derecho a obtener copia gratuita sólo podrá ejercerse personalmente" (art. 12.5). *A contrario sensu*, debemos admitir entonces que los restantes derechos admiten representación.

2. ¿ANTE QUIÉN SE HACEN VALER?

Conforme al artículo 12, los derechos que reconoce la ley se pueden exigir "a quien sea responsable de un banco..." (art. 12.1). Es decir, se ejercen frente a:

- La persona natural que mantenga un registro o banco de datos;
- La persona jurídica de derecho privado que mantenga el mismo registro, o
- Un organismo público que mantenga el mismo registro.

Tratándose de personas naturales o personas jurídicas es claro a quién debe dirigirse la petición. No parece claro el sujeto pasivo si se trata de organismos públicos que carezcan de personalidad jurídica propia. Pareciera que la exigencia debe hacerse a la autoridad superior del respectivo organismo, sin perjuicio de que las acciones

legales que procedan deberán interponerse en contra del Consejo de Defensa del Estado como representante del Fisco.

Debe señalarse que la ley facilita el acceso al conocimiento de registros de organismos públicos, estableciendo a su vez un registro público de dichos registros que queda a cargo del Servicio de Registro Civil e Identificación (art. 22).

Se ha contemplado también el caso de un banco de datos de utilización plural por parte de varias empresas o instituciones. De esta manera, se dispone que si los datos personales están en un banco al cual tienen acceso diversos organismos, "el titular puede requerir información a cualquiera de ellos" (art. 14). Como la norma es restringida a la petición de "información" pensamos que los restantes derechos de modificación, bloqueo y cancelación deberán ejercerse ante el responsable del banco mismo, y no ante alguna de las entidades que tienen acceso a él.

3. FORMAS DE REQUERIMIENTO. GRATUIDAD

La ley no regula la forma en que debe ejercerse el requerimiento, por lo que debemos entender que puede tratarse de petición verbal o escrita, en la que se especifique claramente el objeto de la solicitud: acceso, modificación, bloqueo, cancelación, copia u oposición.

La ley establece la gratuidad en el uso de estos derechos, por lo que el costo que represente su satisfacción deberá soportarlo el respectivo responsable del banco de datos: "La información, modificación o eliminación de los datos serán absolutamente gratuitas" dispone el artículo 12.5 de la ley.

Es curioso que no se haya incluido el derecho a bloqueo dentro de esta enumeración. Interpretada literalmente la norma, opción que parece imponerse por el carácter excepcional de la gratuidad, deberíamos sostener que en caso de bloqueo el costo respectivo debe soportarlo el peticionario.

En cuanto al derecho de copia la gratuidad está condicionada a que transcurra un plazo mínimo de seis meses entre cada ejercicio de este derecho (art. 12.5).

4. IRRENUNCIABILIDAD

Los derechos que establece la ley N° 19.628 son de orden público, ya que se relacionan con la garantía constitucional del respeto a

la vida privada. Esto queda de manifiesto en lo que preceptúa el artículo 13: "El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención".

De esta manera, se prohíbe la exclusión o limitación del ejercicio de estos derechos. Cualquier pacto en contrario adolecerá de nulidad absoluta, conforme a los artículos 10 y 1466 del Código Civil.

De nuevo al legislador se le escapan derechos que no aparecen en esta disposición, como son el derecho de copia del artículo 12.5 y el derecho de oposición del artículo 3º.2. A pesar de la falta de mención en el artículo 13, opinamos que lo mismo debe predicarse de estos derechos, porque no hay razón para hacer diferencias y porque se aplica el mismo principio de que se trata de facultades que tienen el carácter de normas de orden público.

5. CESIÓN Y TRANSMISIBILIDAD

No ha tratado la ley el problema de si los derechos que ella establece son cesibles, a título gratuito u oneroso, o si son transmisibles *mortis causa*.

La cesión de los derechos no parece que pueda ser admitida tratándose de facultades tan esencialmente vinculadas a la persona. Además, no imaginamos en qué supuestos podría un tercero adquirir el derecho de otro para pedir acceso, modificación o cancelación de datos que conciernen al cedente.

Un poco más problemático puede resultar el caso de la transmisión *mortis causa*. ¿Fallecido el titular de los datos, pueden sus herederos ejercer los derechos del artículo 12? El carácter personalísimo de los derechos indicaría una respuesta negativa: los derechos se extinguirían con la persona del titular. Pero es cierto que los herederos pueden tener interés en la rectificación de un asiento relativo a su causante, que puede afectar incluso la posibilidad de obtener créditos para la sucesión.

Pensamos que una solución razonable puede ser considerar que los herederos no pueden actuar ejerciendo el derecho de su causante, puesto que éste ya se ha extinguido, pero sí podrían ejercer esos derechos *iure proprio*, es decir, porque al referirse a su causante los datos han pasado también a afectarles y concernirles; podrán entonces alegar que ellos son ahora los titulares de dichos datos.

IV. EXCEPCIONES

Los derechos de acceso, modificación, bloqueo o cancelación no podrán ejercerse en dos casos de excepción que establece la ley. Éstos son:

1º) Si el ejercicio del derecho impide o entorpece el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido;

2º) Si el ejercicio del derecho afecta la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional (art. 15.1).

Los derechos de modificación, bloqueo o cancelación no pueden además ejercerse respecto de datos almacenados por mandato legal, salvo en los casos contemplados en la ley que ordena ese almacenamiento (art. 15.2). Debe notarse que, respecto de tales registros, procede el derecho a la información o acceso.

V. EL AMPARO DIGITAL O *HÁBEAS DATA*

1. CAUSALES POR LAS QUE PROCEDE

De acuerdo con el artículo 16 de la ley, la acción de amparo procede en dos supuestos:

1º) Si el reponsable del banco de datos no se pronuncia sobre la solicitud del requirente dentro de los dos días hábiles siguientes.

2º) Si el responsable deniega la solicitud. El procedimiento será especial si la causal de denegación es la seguridad de la Nación y el interés nacional.

2. NATURALEZA Y CARACTERES DE LA ACCIÓN

El *habeas data* ha surgido en las últimas décadas prácticamente en todas las legislaciones para otorgar protección expedita al que se ve afectado por el tratamiento de datos de carácter personal, bajo el modelo del recurso de amparo o *habeas corpus* que protege la libertad personal.

Se trata, por tanto, de una acción judicial específica y autónoma, de objeto definido y de tramitación concentrada.

No pensamos que se trate de una acción propiamente cautelar, ya que la sentencia que se dicte producirá cosa juzgada tanto material como formal. Incluso la sentencia incluye la posible aplicación de sanciones.

3. OBJETO DE LA ACCIÓN

La *res petita* en la acción de *habeas data* es según la ley el "amparo a los derechos consagrados en el artículo precedente" (art. 16.1). El artículo anterior, el 15, menciona los derechos de información, modificación, bloqueo y cancelación. Cualquiera de ellos puede ser objeto de la acción de amparo digital.

No son mencionados en el artículo 15 los derechos de copia y de oposición. No parece haber razón para excluirlos de esta protección específica. Respecto del derecho de copia, puede decirse que está implícito en el artículo 15 ya que nace del ejercicio del derecho de modificación o cancelación.

Este recurso interpretativo no podemos aplicarlo al derecho de oposición que establece el artículo 3º.2, por lo que parece quedar excluido del ámbito de protección que brinda esta acción. Ello no obsta para que el derecho pueda ejercerse mediante una acción ordinaria de responsabilidad civil o mediante la acción constitucional de protección.

Pero aparte del amparo de los derechos referidos, la acción puede tener por objeto además la indemnización de los perjuicios causados (art. 23) y la constatación de una responsabilidad infraccional sobre la que proceden sanciones administrativas (art. 16 *in fine*).

4. TRIBUNAL COMPETENTE

La competencia corresponde al juez de letras en lo civil del lugar del domicilio del responsable del banco de datos.

Aunque en la tramitación de la ley se pensó en dar más facilidades al particular afectado otorgando competencia al tribunal de su propio domicilio, primó la opinión de que debían mantenerse las reglas generales de competencia que privilegian el domicilio del demandado (art. 134 COT).

5. LEGITIMACIÓN ACTIVA Y PASIVA

La acción puede interponerse sólo por el "titular de los datos" (art. 16.1). De nuevo, hacemos la advertencia que si se trata del derecho de acceso o información la acción podrá interponerse por cualquier persona que tema estar incluida en la respectiva base de datos personales.

Lo que hemos dicho anteriormente en cuanto a la representación, a la cesión y la transmisión de estos derechos, resulta plenamente aplicable para el ejercicio de la acción que los ampara.

La acción debe interponerse contra el responsable del registro o banco de datos. Si se trata de persona jurídica habrá que demandar a quienes ostenten su representación judicial; si se interpone respecto de un organismo público sin personalidad jurídica propia habrá que emplazar al Consejo de Defensa del Estado.

6. PROCEDIMIENTO

a) Reclamación de amparo

La reclamación debe señalar la infracción cometida y los hechos que la configuran. Entendemos que para la ley el no respeto de los derechos por ella concedidos es suficiente para hablar de infracción a sus normas. Aunque la ley no lo diga expresamente, se deduce que la reclamación ha de ser escrita.

Además, la reclamación debe ir acompañada "de los medios de prueba que los acrediten, en su caso" (art. 16, letra a). La expresión "en su caso" denota que este requisito no es perentorio y que dependerá de la naturaleza de la infracción el que existan o no medios de prueba que puedan acompañarse.

b) Notificación y contestación

La reclamación debe notificarse por cédula dejada en el domicilio del responsable del banco de datos (art. 16, letra c). No parece oportuno haber hecho excepción a la regla general de que la primera notificación debe hacerse personalmente.

El plazo para que el banco de datos conteste, presentando sus descargos, es de cinco días hábiles desde la notificación. La contestación será también hecha por escrito, y a ella deben acompañarse

los medios de prueba que acrediten los hechos en los que se funda (art. 16, letra b).

c) Audiencia de prueba

Si el banco de datos no dispone de medios de prueba para acompañar en su contestación, debe indicar en ella esta circunstancia y el juez fijará una audiencia dentro del quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada (art. 16, letra c).

Pensamos que esta audiencia también debe practicarse cuando sea el requirente el que no haya podido acompañar en la reclamación sus medios de prueba, si expresa esta circunstancia y ofrece rendir prueba.

d) Sentencia

La sentencia definitiva debe dictarse dentro del tercer día hábil de vencido el plazo para contestar, se hayan o no presentado descargos, o desde que vence el plazo fijado para la audiencia de prueba (art. 16, letra d).

La sentencia definitiva debe notificarse por cédula (art. 16, letra b).

e) Recursos

Las resoluciones dictadas en el proceso se notifican por el estado diario y no son apelables (art. 16, letra e).

La sentencia definitiva es apelable en ambos efectos. El recurso de apelación debe interponerse en el plazo de cinco días (aunque la ley no lo diga debemos entender hábiles) desde la notificación de la parte que entabla el recurso. El escrito de la apelación deberá contener los fundamentos de hecho y de derecho y las peticiones concretas que se formulan (art. 16, letra f). Al decir esto, la ley no hace más que repetir a la letra el artículo 189 inciso primero del Código de Procedimiento Civil

La ley agrega que el Presidente de la Corte de Apelaciones debe ordenar dar cuenta preferente del recurso, sin esperar la comparencia de las partes (art. 16, letra g). En principio, el recurso se ve en cuenta, pero la Sala que debe conocer, si lo estima conveniente o se le solicita con fundamento plausible, puede ordenar traer los autos en relación para oír los alegatos de los abogados de las

partes. En tal caso, la causa se agrega extraordinariamente a la tabla de la misma sala (art. 16.4).

La sentencia de segunda instancia no es susceptible de los recursos de casación (art. 16, letra h). Parece que procedería entonces el recurso de queja, conforme con lo dispuesto en el artículo 545 del Código Orgánico de Tribunales.

f) Procedimiento especial en caso de seguridad de la Nación o interés nacional

Si la causal que el responsable de los datos ha invocado para denegar la solicitud del requirente es la seguridad de la Nación o el interés nacional, la reclamación debe deducirse directamente ante la Corte Suprema.

La Corte debe pedir informe al responsable del modo más expedito y le fijará un plazo. Vencido el plazo resolverá en cuenta.

Si se recibe la causa a prueba, ésta debe consignarse en un cuaderno separado y reservado. Este cuaderno mantendrá el carácter de reservado si la reclamación es denegada (art. 16.3).

La sala de la Corte Suprema puede también, si lo estima conveniente o se le solicita con fundamento plausible, ordenar traer los autos en relación, caso en el cual la causa se agrega extraordinariamente a la tabla. Pero el Presidente de la Corte debe disponer que la audiencia no sea pública (art. 16.5).

7. CONTENIDO Y EJECUCIÓN DE LA SENTENCIA

La sentencia que acoge la reclamación el juez debe fijar un plazo prudencial para que el banco de datos dé cumplimiento a lo resuelto.

Además puede sancionar la infracción con una multa de una a diez unidades tributarias mensuales (art. 16.5) y determinar los perjuicios si le han sido solicitados (art. 23).

En caso de que el responsable no cumpla dentro del plazo en la forma que decreta el tribunal, puede aplicar multas de dos a cincuenta unidades tributarias mensuales. Y si el requerido es un organismo público, el juez puede sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

Las sanciones son realmente muy poco significativas.

VI. RESPONSABILIDAD CIVIL Y DERECHO A LA INDEMNIZACIÓN DE PERJUICIOS

1. NATURALEZA DE LA RESPONSABILIDAD

El artículo 23 de la ley establece que la persona natural o jurídica privada o el organismo público responsable del banco de datos debe indemnizar los perjuicios 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 o, en su caso, lo ordenado por el tribunal.

Como la ley no establece mayores precisiones sobre esta responsabilidad, debemos indagar sobre su naturaleza para ver cuáles reglas del derecho común le son aplicables.

En primer lugar, hay que dilucidar si estamos frente a una responsabilidad contractual o extracontractual. La respuesta no puede ser sino que se trata de un supuesto de responsabilidad extracontractual. Aunque la presencia de una autorización expresa y por escrito de un titular de datos para la utilización de éstos podría hacer surgir dudas sobre si hay un contrato que fija el marco de actuación entre las partes, pensamos que dicha autorización es un acto unilateral y no la aceptación de un acuerdo contractual. Por lo demás, la ley se refiere a la responsabilidad civil como aneja a la responsabilidad infraccional (art. 23.2), lo que sólo se condice con la responsabilidad civil extracontractual.

En lo no previsto, por lo tanto se aplicarán las normas de los artículos 2314 y siguientes del Código Civil.

Una segunda cuestión es la relativa al factor de imputación de la responsabilidad: ¿estamos aquí frente a un nuevo supuesto de responsabilidad objetiva, respecto del cual el perjudicado sólo debe probar los perjuicios, el acto injusto y el nexo de causalidad pero no la culpa o dolo del agente? De la expresión perentoria que aparece en el artículo 23: "deberá indemnizar", alguien podría deducir que estamos ante un caso de objetivación de la responsabilidad. Nos parece que ello no es así, por varias razones:

1º) El régimen común de la responsabilidad es el principio de la culpa, y para que haya excepción a este principio debe existir una norma inequívoca al respecto.

2º) La expresión "deberá indemnizar" no dice más que, cumplidos los presupuestos de la responsabilidad, nace la obligación de indemnizar.

3º) La responsabilidad civil en el artículo 23 aparece como aneja a la infracción legal, y ésta no puede existir sin negligencia o culpa. No hay responsabilidad contravencional sin dolo o culpa.

4º) La historia de la tramitación de la ley confirma esta conclusión, pues consta que se agregó el calificativo de "indebido" al tratamiento de datos que produce responsabilidad, justamente para enfatizar la necesidad de la aplicación de las reglas generales de la responsabilidad por culpa. Se lee en el Informe de la Comisión Mixta: "La Comisión Mixta estimó 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 por el Código Civil".

2. PERJUICIOS INDEMNIZABLES

El artículo 23 aclara que se puede obtener indemnización de todos los perjuicios causados por el tratamiento indebido de los datos, incluyéndose tanto la reparación de los daños materiales como de los daños morales.

Debe considerarse que ya al realizarse la modificación o cancelación de los datos hay una forma de reparación de los daños, y que si se pretende obtener una indemnización adicional deberán probarse estos perjuicios, incluso los morales. El juez apreciará esta prueba en conciencia (art. 23.2).

3. TRIBUNAL COMPETENTE Y PROCEDIMIENTO

La acción para solicitar indemnización de perjuicios puede deducirse conjuntamente con la de amparo del artículo 16 ante el mismo tribunal y con el mismo procedimiento regulado para conocer de ella. Procede en este caso diferir la discusión sobre el monto de los perjuicios en la ejecución del fallo o en otro juicio, de acuerdo con el artículo 173 del Código de Procedimiento Civil (art. 23.1).

Si la responsabilidad surge por una conducta infraccional que no es de las señaladas en el artículo 16 (y en el art. 19 que se remite a él), según el artículo 23.2, debe aplicarse el procedimiento sumario tanto para el establecimiento de la infracción como para la indem-

nización de perjuicios. No se indica quién es el juez competente ni tampoco las sanciones que proceden por estas infracciones no mencionadas en los artículos 16 y 19, por lo que vemos muy difícil que pueda articularse esta responsabilidad.

Podría sí ejercerse en forma separada la acción de responsabilidad civil, y en ese caso será competente el juez de letras en lo civil del domicilio del demandado y se aplicará el procedimiento sumario (art. 23.2).

4. MEDIDAS CAUTELARES

El artículo 23.2 dispone que “el juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece”.

Parece curioso que esta norma relativa al amparo de los derechos se encuentre en el artículo que regula la responsabilidad civil, pues debió haberse dispuesto en general para todos los procedimientos.

VII. DERECHOS DE LOS TITULARES DE DATOS Y LA PROTECCIÓN A LA VIDA PRIVADA

1. ¿UN ÚNICO DERECHO DE FACULTADES DIFERENCIADAS?

Analizada ya la preceptiva de la ley, se nos presentan varias cuestiones de interés teórico, pero con repercusiones prácticas.

En primer lugar, hay que resolver si estamos frente a un único derecho de protección de datos personales o ante un haz de derechos diversos y autónomos entre sí.

La cuestión tiene relieve práctico pues si se trata de un derecho único, aunque con diversas modalidades de ejercicio o facultades, la petición de una de estas modalidades de ejercicio incluye necesariamente las otras, si es del caso. En cambio, si se trata de derechos diferentes, debe plantearse una acción para cada derecho. En el primer caso, la sentencia producirá cosa juzgada sobre todas las modalidades de aplicación del derecho; mientras que en el segundo ella sólo se aplicará a la facultad concreta que se discutió en el juicio.

En nuestra opinión, se trata de derechos diferentes, aunque todos ellos tienen en común la finalidad de proteger un interés

jurídico común: la protección de la intimidad e identidad frente al tratamiento de datos personales. Solamente el derecho de copia puede conceptualizarse como una facultad derivada de los derechos de modificación o eliminación.

2. ¿DERECHOS DIVERSOS CON TUTELA UNIFICADA?

La tutela judicial a través de una sola acción de amparo no necesariamente obliga a pensar que estamos frente a un solo derecho, siguiendo la regla clásica de que a todo derecho corresponde una acción.

La acción de amparo digital o *habeas data* es una forma de tutela judicial amplia que cubre la protección de un conjunto de derechos que, aunque con fisonomías propias, tienen en relación que responden al mismo interés.

3. ¿APLICACIÓN O COMPLEMENTACIÓN DE LA GARANTÍA CONSTITUCIONAL DEL RESPETO A LA VIDA PRIVADA?

Nos queda por determinar si los derechos que reconoce la ley N° 19.628 a los particulares son aplicaciones particulares del derecho al respeto y protección de la vida privada consagrado en el artículo 19, N° 4 de la Carta Fundamental, o si, por el contrario, vienen a complementar esa preceptiva innovando así en la protección del individuo.

Debe señalarse en abono de la segunda opinión que en varias Constituciones se prescribe en forma especial el derecho al amparo digital o *habeas data*.

La tramitación de la ley, que partió como una normativa dirigida a proteger el derecho a la intimidad y se convirtió finalmente en una ley de protección de datos, nos habla también de este problema. La dicotomía de objetivos se advierte en su publicación en el Diario Oficial en el que curiosamente se alude a la ley "sobre protección de la vida privada", en tanto que el decreto de promulgación señala que el proyecto de ley sancionado se titula "protección de datos de carácter personal".

Pareciera que, si bien en parte los derechos de la ley N° 19.628 son formas de aplicación del derecho general al respeto a la vida privada, en cuanto permiten excluir datos que se refieren al ámbito de intimidad que una persona razonablemente reserva para sí y su entorno familiar, por otro lado, también sirven para resguardar el

llamado “derecho a la identidad”, que no está como tal contemplado en el artículo 19 N° 4 de la Constitución, pero que puede caber en la alusión que hace el precepto al respeto de la “vida pública” de la persona. Los derechos de modificación tienden muchas veces a resguardar este derecho a la identidad en la vida pública, más que el derecho a la intimidad.

Por las razones expuestas, el recurso de protección que el artículo 20 de la Constitución reserva para las amenazas, privaciones o perturbaciones del derecho al respeto y protección a la vida privada puede interponerse en los casos de infracciones a la ley 19.628 si el atentado al derecho se comete a través del tratamiento de datos de carácter personal. La deducción del recurso y su fallo no obstará a que posteriormente el particular pueda ejercer la acción de amparo digital o *habeas data*, ya que el artículo 20 de la Constitución señala expresamente que la acción constitucional es “sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes”. Se aplicará lo mismo que sucede con el llamado amparo económico.

Para aquellos atentados que no son dirigidos propiamente a la vida privada, sino que tienden a distorsionar la presentación de la persona en la vida social, procederá también, a nuestro juicio, el recurso de protección, esta vez por afectación del derecho al respeto a la vida pública, sin perjuicio de la procedencia igualmente del amparo digital que establece la ley N° 19.628. Para el caso de no considerarse procedente la interpretación que hacemos de la locución “vida pública” del artículo 19 N° 4 de la Constitución, la acción de la ley N° 19.628 será el único medio jurisdiccional de que disponga el afectado para resguardar el derecho a su identidad.

La tutela de la información digitalizada como una forma especial de protección a la vida privada y como un complemento a ella (derecho a la identidad) debe considerarse un paso positivo en la configuración de recursos efectivos que resguarden a las personas de los peligros que enfrentan ante una utilización abusiva y dañina de las nuevas tecnologías del mercado de la información.



RÉGIMEN DE LOS DATOS DE CARÁCTER ECONÓMICO, FINANCIERO, BANCARIO O COMERCIAL EN LA LEY N° 19.628

RONY JARA AMIGO
Profesor de Derecho Comercial
Universidad de los Andes

I. INTRODUCCIÓN

Este trabajo aborda un tema que en esta sociedad de la información y economía de mercado en la que vivimos ha adquirido una importancia creciente: el tratamiento de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, materia que es regulada fundamentalmente en el Título III de la Ley N° 19.628. Su tratamiento estará dividido en las siguientes partes:

1. Algunos conceptos económicos y constitucionales básicos;
2. Experiencia del derecho y de la doctrina comparada y de la jurisprudencia nacional;
3. Análisis de algunos elementos fundamentales en la ley;
4. Algunos problemas y posibles soluciones.

II. ALGUNOS CONCEPTOS ECONÓMICOS Y CONSTITUCIONALES BÁSICOS

El tema de las bases de datos puede ser analizado desde múltiples perspectivas, sólo es preciso aquí mencionar dos, estrechamente vinculadas con el tema a desarrollar: la cuestión de lógica económica y la de algunos derechos constitucionalmente protegidos.

1. ASPECTOS ECONÓMICOS

En relación al tema económico es interesante destacar los siguientes aspectos:

- i) Un adecuado nivel de producción de la información;
- ii) El rol de la información en la determinación de los riesgos y la fijación de los precios;
- iii) Información y economía del consumo.

Respecto de lo primero, es decir el nivel de producción óptimo de la información —en este caso representado por la producción de bases de datos comerciales— sabemos que la información es un bien de aquellos que los economistas denominan “bienes públicos” puesto que su consumo por una persona no excluye el consumo por otra, de modo que puesta en el mercado, muchas personas pueden beneficiarse de ella por un precio que en el óptimo debiera ser cero. Entonces el problema de estos bienes, por una parte, es que si no 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 produciría¹.

El legislador de la Ley N° 19.628 ha reconocido como regla general, con algunas excepciones importantes, un sistema de libertad empresarial para la creación de bases de datos comerciales, lo que unido a un sistema de protección de la autoría de la base de datos o de monopolio legal debiera asegurar una producción más o menos adecuada de la información que es permitido comunicar. Probablemente, los problemas se van a producir, por una parte, respecto de la información que no se puede comunicar, existiendo demanda por ella, lo que siempre crea incentivos económicos ineficientes para tratar de burlar esa prohibición, y, por otra, los relati-

¹ Sergio Cámara Lapuente, “Últimas Orientaciones Internacionales Sobre la Protección Jurídica de las Bases de Datos”, Rev. Chilena de Derecho, Vol. 26 N° 1 (1999), p. 31-32.

vos a la formación de ciertas empresas con posiciones dominantes en la producción o comunicación de la información. ¿Por qué pudiera darse esto último existiendo libertad de producción? Porque existen determinadas fuentes de producción de la información que se encuentran legal o reglamentariamente vinculadas con ciertas bases de datos y ello puede constituir una importante barrera de entrada para la existencia de otros bancos de datos, en especial cuando la información que se puede comunicar es casi exclusivamente la que aquella base de datos legal obtiene de sus fuentes vinculadas. Puede haber, entonces, un consumo subóptimo de información comercial.

En relación al segundo tema económico, durante la tramitación del proyecto de ley, numerosas entidades —asociaciones de aseguradores, de prestadores de servicios de salud, etc.²— plantearon al legislador la relación entre información y riesgo, argumentando que mientras mayor era la información con 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 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”.

Por último, es del caso señalar que esta mayor información le permite al oferente de un bien o servicio discriminar entre sus potenciales consumidores, y decidir si contratar o no, en qué condiciones hacerlo o qué precios cobrar a cada uno de ellos. Desde la perspectiva individual del oferente ello aparece entonces conveniente, puesto que asocia mejor riesgo y precio, y puede también serlo para el consumidor, porque —como se ha señalado ya— le podrá dar la oportunidad de acceder a un precio más conveniente, dada su historia personal, que aquel general que, en otro caso, debiera asumir. En todo caso, es necesario añadir que este razona-

² Boletín 896-07, Informe de Comisión Mixta relativo al proyecto de ley sobre protección de datos de carácter personal.

miento individual tiene sus limitaciones en el agregado, porque sabemos que la posibilidad de elevar los precios por la falta de posibilidad de discriminar es limitada fuertemente —en muchos mercados— por el nivel de competencia existente en ellos. De esta forma, muchos oferentes y consumidores, en mercados competitivos, son verdaderos tomadores de precios³, y los sistemas de administración de los riesgos basados en portafolios y estadísticas, precisamente se basan en ello.

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 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, porque lo propio de ella es asumir riesgo y si se fracasa será conveniente que después de transcurrida cierta cantidad de años, esa persona pueda tener nuevamente la posibilidad de desarrollar su actividad profesional. 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 en dicha actividad económica.

2. ASPECTOS CONSTITUCIONALES

En materia de aspectos constitucionales sólo es del caso poner de relieve algunas cuestiones que parecen básicas para la comprensión del marco general en el cual se inserta la normativa legal en materia de datos personales de carácter comercial. Así, sólo se comentará lo siguiente:

- i) La diferencia entre el derecho a la vida privada y el derecho a la honra;

³ Esto significa que aquellos oferentes y consumidores enfrentan un precio dado para todo el mercado respecto de los bienes o servicios que ofrecen o consumen, respectivamente, el cual no varía por su comportamiento particular de oferta o consumo.

- ii) La coordinación entre distintas garantías constitucionales;
- iii) La información con carácter supraindividual.

El derecho a la vida privada dice relación con la tutela de la intimidad; o en otras palabras, con una barrera opuesta a la entrada de un individuo en el círculo de confianza de otra persona. Así, se supone que toda persona tiene derecho en forma exclusiva y excluyente a hacer públicas ciertas manifestaciones de su vida privada, cuando lo estime conveniente. Este derecho, tiene una estrecha relación con la información que se contenga en los bancos de datos, puesto que ellos pueden dar cuenta de informes íntimos, de comportamientos personales, de elementos distintivos de la personalidad, en fin, de una verdadera "identidad informática" que debería otorgar derechos a su titular. Entre los datos que pudieran encontrarse cubiertos por ella se encuentran los relativos a los comportamientos comerciales.

Por otra parte, el derecho de una persona al honor se refiere al derecho a no ser ofendido en su fama. Es decir, en este caso para que exista atentado se requiere que la persona sea infamada, en cambio un atentado al derecho a la vida privada no supone ofensa a la fama, sino infracción al control que corresponde a todo individuo sobre los datos referentes a su propia persona. Así, se puede señalar que la protección del derecho a la vida privada es más exigente, por cuanto el solo comunicar ciertos datos personales podría implicar una violación de la intimidad, en cambio respecto de la protección a la honra se requerirá que los datos sean falsos o se refieran a ciertas materias que por su solo conocimiento por terceros pueda causar el descrédito de la persona afectada⁴. Los antecedentes comerciales, en ciertos casos, pudieran afectar el buen nombre de su titular.

Con respecto a la coordinación entre distintas garantías constitucionales, la doctrina y jurisprudencia están relativamente de acuerdo en que no existen derechos absolutos y que cada vez que se produce una colisión de derechos es necesario armonizar su aplicación, lo que puede implicar que algunos de ellos se subordinen a los otros en determinadas situaciones, y viceversa, en otros casos.

⁴ José Luis Cea Egaña: *El Sistema Constitucional de Chile* (Valdivia, Facultad de Ciencias Jurídicas y Sociales de la Universidad Austral, 1999) pp. 94 y 174; Enrique Evans de la Cuadra: *I Derechos Constitucionales* (Santiago, Ed. Jurídica de Chile, 1986), pp. 171-176.

Pues bien, en este caso se plantea una aparente contradicción entre el derecho a la vida privada y a la honra y la libertad de información. La doctrina y jurisprudencia nacional han señalado que tratándose de vida privada debe, en principio, primar el derecho a la intimidad frente a la libertad de información⁵. Pero también ha indicado que esa regla tiene excepciones, puesto que el secreto de lo íntimo no puede invocarse para encubrir el dolo propio o lesionar el bien común⁶.

En relación con lo anterior, se debe mencionar lo que ha venido en denominarse "datos supraindividuales", esto es, datos que no son ni sensibles ni afectan la intimidad o vida privada, puesto que trascienden la esfera íntima del sujeto o su familia para situarse en el ámbito de lo que puede y, en ciertos casos, debe ser conocido por terceros⁷.

III. EXPERIENCIA DEL DERECHO Y DOCTRINA COMPARADA Y DE LA JURISPRUDENCIA NACIONAL

Con respecto al derecho extranjero es pertinente referirse brevemente a algunas legislaciones que han regulado la materia.

Así, en el caso de México⁸, la norma legal respectiva ha regulado sólo la información que se encuentra cubierta por secreto bancario y ha establecido que el principio básico para la utilización de dicha información es contar con la autorización expresa y por escrito del titular de los respectivos datos.

En España⁹, el legislador ha establecido el principio que los datos personales de personas físicas sólo pueden ser sometidos a tratamiento cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para

⁵ Considerando 3º de la sentencia pronunciada por la Corte Suprema el 15 de junio de 1993 (Rol N° 21053), y considerando 8º de la sentencia de la Corte de Apelaciones de Santiago pronunciada el 31 de mayo de 1993, confirmada por la Corte Suprema el 15 de junio de 1993. En la doctrina, Sergio Díez Urzúa: *Personas y Valores* (Santiago, Ed. Jurídica de Chile, 1999) pp. 148-156.

⁶ J.L. Cea, *Gaceta Jurídica* N° 194 (1996) p. 33.

⁷ Recurso de Inconstitucionalidad presentado por Dicom S.A. ante el Tribunal Constitucional con fecha 19 de julio de 1999, p. 10.

⁸ Art. 33º de la Ley para Regular las Agrupaciones Financieras, Diario Oficial de la Federación de los Estados Unidos Mexicanos, 15 de febrero de 1995.

⁹ Ley Orgánica N° 5 de 29 de octubre de 1992 sobre Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

las que se hayan obtenido¹⁰. Además, si bien el principio que impera es que el tratamiento de los datos requiere el consentimiento del afectado, la norma ha establecido varias excepciones, entre las cuales se encuentran los casos en que los datos personales se recojan de fuentes accesibles al público, o cuando se refieran a personas vinculadas por una relación comercial o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato¹¹. De este modo, se han conjugado armoniosamente los intereses del afectado con los que tienen carácter supraindividual.

En Alemania¹², la norma legal ha señalado que es posible el tratamiento de datos personales: i) dentro del marco del fin y objeto de una relación contractual o de confianza, constituida con el afectado; ii) si fuere necesario para salvaguardar justos intereses del organismo almacenante y no existiese motivo fundado para creer que prevalece el interés legítimo del afectado en contra de su elaboración o uso; iii) si los datos fueren tomados de fuentes accesibles con carácter general (...), a menos que prevaleciere manifiestamente el interés legítimo del afectado (...)¹³. Asimismo, la norma agrega que será lícito ceder o usar datos si fuere necesario para salvaguardar justos intereses de un tercero o el interés público¹⁴. De esta forma el legislador ha armonizado los derechos del titular de los datos con el de terceros, el público y la comunidad en general.

Por último, parece útil destacar la normativa del Parlamento y Consejo de Europa¹⁵. En ella se señala que es posible el tratamiento de los datos personales, entre otros casos, si el interesado otorga su consentimiento; si es necesario para la ejecución de un contrato en que el interesado sea parte o para la aplicación de medidas precontractuales; si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado (...). Así, también se ha alcanzado un adecuado equilibrio de los intereses respectivos, entre el titular de los datos y los de los terceros.

¹⁰ Id. artículo 4°.

¹¹ Id. artículo 2°.

¹² Ley Alemana Federal de Protección de Datos de 20 de diciembre de 1990.

¹³ Id. artículo 28°.

¹⁴ Id. artículo 29°.

¹⁵ Directiva N° 95/46/CE del Parlamento y Consejo de Europa de 24 de octubre de 1995, publicada en el Diario Oficial de las Comunidades Europeas de 23 de noviembre de 1995.

En general, la doctrina comparada se ha inclinado por la protección de los datos informatizados, pero no en términos absolutos o de una facultad de autodeterminación ilimitada, del respectivo titular, para disponer de ellos a su discreción. En general, se ha hecho fundamental determinar por dónde discurre el límite entre lo auténticamente privado y aquello que afecta legítimos intereses de terceros. Puesto que incluso el comportamiento personal en la esfera más íntima puede tener relevancia social.

Así, por ejemplo, cierta doctrina argentina ha excluido del *hábeas data* algunos datos que, con suficiente razonabilidad, son de interés público o general; por ejemplo, la información que se refiere a la actividad comercial, empresarial o financiera de las personas, porque su conocimiento parece de acceso necesario a terceros que también están insertos en la red de similares actividades¹⁶.

Con respecto a la jurisprudencia nacional, si bien ella no ha hecho un tratamiento acabado y profundo del tema, es posible distinguir algunos principios que se han ido reiterando durante los últimos años:

1. Las sentencias —dictadas mayoritariamente en recursos de protección y en menor medida frente a demandas de indemnización de perjuicios, que buscaban terminar con la publicación de antecedentes comerciales de los demandantes o ser indemnizados por tales actos, respectivamente— han sido consistentes en rechazar las acciones deducidas, sobre la base que se trataba de datos informatizados obtenidos en fuentes abiertas o públicas. Si dichas fuentes eran oficiales, el principio ha sido absoluto, en cambio si no lo eran, en ciertos casos ha existido una cierta presunción de veracidad de la información a favor del dueño de la base de datos¹⁷ y en otros, los tribunales han señalado que se infringe el derecho a la intimidad y a la honra en los casos de no haberse verificado a cabalidad la efectividad de las informaciones comerciales difundidas¹⁸;

2. De esta forma, frente a una posible antinomia entre el derecho al respeto y protección de la honra de la persona y la libertad

¹⁶ Germán J. Bidart Campos: II Manual de la Constitución Reformada (Bs. Aires, Ediar, 1997), p. 390.

¹⁷ Corte Suprema, 10 de Junio de 1998, causa Rol 1789-98.

¹⁸ Corte de Apelaciones de Puerto Montt, 18 de marzo de 1997, confirmada por la Corte Suprema, 16 de julio de 1997, causa Rol 893-97.

de emitir opinión y de informar, se ha hecho primar esta última, siempre que se haya ejercido responsablemente, es decir, que la información sea veraz¹⁹;

3. Se ha señalado reiteradamente que la publicación de información comercial no es una actividad empresarial que sea contraria a las leyes, orden público o seguridad interior;

4. Con respecto a la vigencia de la información comercial, se ha resuelto que la pérdida de la vigencia de un hecho comercial, como es el protesto de un documento, no supone la eliminación de una base de datos²⁰, sino sólo que las instituciones financieras no pueden considerar dicha información, por especial disposición de la autoridad fiscalizadora²¹;

5. Por otra parte, y con especial referencia a la vida privada y la honra, se ha señalado que la publicación de hechos de carácter patrimonial y comercial quedan fuera del ámbito de la vida familiar e íntima de las personas²² y también que, "la conducta financiera y comercial, que guarda estrecha vinculación con las actividades económicas que el actor realiza dentro del grupo social en que aquéllas se desenvuelven, necesariamente deben ser de conocimiento de las personas naturales y jurídicas con quienes se vincula, lo que excluye la idea de privacidad (...) y por consiguiente los datos computacionales de cuya divulgación reclama son realidades ocurridas durante cierto tiempo de su actividad financiera"²³;

6. Por último, es preciso destacar que se ha reconocido el daño causado por el dueño de una base de datos en los casos de publicación de información sin la correspondiente verificación de identidad de las personas afectadas²⁴ y que una persona tiene

¹⁹ Id.

²⁰ Corte de Apelaciones de Santiago, 16 de octubre de 1996, causa Rol 3.041-96, confirmada por la Corte Suprema, 17 de marzo de 1997, causa Rol 3.986-96.

²¹ Capítulo 20-6 de la Recopilación de Normas de la Superintendencia de Bancos e Instituciones Financieras.

²² Corte de Apelaciones de Valdivia, 31 de julio de 1997, causa Rol 8.023-97, confirmada por la Corte Suprema, 24 de septiembre de 1997, causa Rol 2.662-97.

²³ Corte de Apelaciones de Santiago de 2 de abril de 1991, causa Rol 47-91.

²⁴ Corte de Apelaciones de Concepción, 9 de julio de 1998, causa Rol 23-98, confirmada por la Corte Suprema, 27 de agosto de 1998, causa Rol 2509-98.

derecho a indemnización de perjuicios por el menoscabo y desprestigio comercial que le ha causado el protesto equivocado por un acreedor de una letra de cambio y la publicación del mismo²⁵.

IV. ANÁLISIS DE ALGUNOS ELEMENTOS FUNDAMENTALES DE LA LEY N° 19.628

En relación al contenido de la ley 19.628 es apropiado destacar ciertos aspectos que son básicos para comprender la esencia de la regulación. Así cabe mencionar:

1. Los conceptos de dato personal y de dato sensible. El dato personal de contenido comercial como una categoría intermedia;
2. Los conceptos de tratamiento y comunicación de datos;
3. La relación entre los principios generales de la ley y aquellos particulares;
4. La analogía entre los datos personales comerciales y los relativos a sanciones penales o administrativas.

1. LOS CONCEPTOS DE DATO PERSONAL Y DE DATO SENSIBLE.

EL DATO PERSONAL DE CONTENIDO COMERCIAL COMO UNA CATEGORÍA INTERMEDIA

La ley en comento ha establecido una clara distinción entre el género de los datos personales, señalando que es aquel relativo a cualquier información concerniente a personas naturales, identificadas o identificables (letra f) del art. 2°), con la especie de los datos sensibles, pues esta clase de datos personales se refiere a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad (letra g) del art. 2°). Es decir, estos últimos claramente y en todo caso se encuentran dentro del ámbito de la vida privada o intimidad, por lo que su tratamiento normativo es diferente. Así, la ley es mucho más restrictiva en relación con el tratamiento de los datos sensibles, pero presenta el principio en forma bastante similar, pues en el caso de

²⁵ Corte de Apelaciones de Concepción, causa Rol 697-89, confirmada por la Corte Suprema, 7 de mayo de 1992, causa Rol 1.072-92. En este caso se trata de daño moral a una sociedad comercial.

los datos personales, la ley señala que su tratamiento sólo puede efectuarse cuando la ley o el respectivo titular consienta en ello (art. 4º), y en el caso de los datos sensibles la norma prohíbe su tratamiento, salvo cuando la ley o el respectivo titular consienta en ello (art. 10).

La diferencia viene dada por el lado de las excepciones, puesto que en el caso de los datos sensibles la única excepción a la regla general está dada por la necesidad de su tratamiento "para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares" (art. 10), lo que, entre otros efectos, permite determinar la razón riesgo/precio de los que aseguran la prestación de servicios de salud. En cambio, en el caso de los datos personales, la ley plantea importantes y amplias excepciones en el caso de los datos que provengan o que se recolecten de fuentes accesibles al público. Así, en dichos casos, releva de la autorización del titular: (i) cuando sean de carácter económico, financiero, bancario o comercial; (ii) se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes de individualización de la persona, o (iii) sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. También, en el caso de los datos personales, la Ley contempla una importante excepción —según se verá— que permite su tratamiento por parte de personas jurídicas privadas para uso exclusivo de dichas entidades y ciertas personas vinculadas (art. 4º). En todo caso, es preciso señalar que en todos los casos —tratándose de datos personales o sensibles— si la fuente de la autorización para el tratamiento ha sido el consentimiento del titular, esa autorización puede ser revocada en cualquier tiempo sin efecto retroactivo. Además, 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 (art. 4º).

A la luz de lo expuesto, parece aparentemente claro que los datos de contenido económico, financiero, bancario o comercial pertenecen al género de los datos personales y no a la especie de los sensibles. La propia ley, en el referido artículo 4º, asienta el principio general que permite tratarlos cuando provengan o se recolecten de fuentes accesibles al público. Estas fuentes, como se define en la ley, son aquellas recopilaciones de datos personales,

públicos o privados, de acceso no restringido o reservado a los solicitantes (letra i) del art. 2º). Sin embargo, la lógica seguida por el artículo 17º, que señala un listado taxativo de los datos de contenido comercial que pueden ser comunicados, descartando en consecuencia aquellos no incluidos, pareciera configurar a los datos comerciales en una especie distinta de los sensibles, pero que tampoco se identifica totalmente con el género, puesto que su comunicación, al menos, sería mucho más restrictiva.

En principio, no se divisan razones en el sistema jurídico o en la propia ley para construir esta categoría especial de datos personales. En el sistema jurídico, por cuanto como ha quedado demostrado, por la referencia al derecho y doctrina comparada y a la jurisprudencia nacional, se ha entendido 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 sobre la protección de la intimidad. Tampoco en la propia ley, pues en ella el principio de autodeterminación informativa se construye en función de los datos sensibles o personalísimos, donde el legislador ha sido extremadamente estricto en la tutela de la vida privada, pero en el caso de los datos comerciales esa razón no existe; en ellos no existe la facultad de autodeterminación y, por el contrario, si surge un conflicto debería prevalecer el interés supraindividual, traducido en la libertad de informar, porque allí no hay secreto legítimo²⁶.

En la propia Comisión Mixta,²⁷ en la cual se incorporó esta categoría especial, se debatió sobre las posibilidades normativas. Por una parte, podía establecerse un sistema de amplia libertad de información en materia de datos comerciales, fundado en el adecuado funcionamiento de la actividad económica y el legítimo interés de terceros. Dicho sistema debía tener como contrapeso mecanismos que resguardaran el carácter fidedigno de la información y un procedimiento que ofreciese ciertas garantías de seriedad, al cual debían sujetarse los acreedores para comunicar información a los responsables de las bases de datos. En nuestra opinión, esa era la opción compatible con el sistema jurídico y con el resto del texto legal. Sin embargo, se optó por la otra alternativa,

²⁶ Recurso de Inconstitucionalidad, p. 21.

²⁷ Boletín 896-07.

esto es, señalar de modo taxativo las obligaciones impagas de carácter comercial que podían ser tratadas en un banco de datos, con exclusión de cualquiera otra. Esta alternativa se fundó 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 íntimo, su menor trascendencia, su dudoso fundamento o exigibilidad, etc."²⁸ En consecuencia —en aquellos datos excluidos de la nómina— se impuso el derecho a la intimidad por sobre el derecho a la información, aun cuando se tratara de datos supraindividuales.

Al parecer, pesó mucho en nuestro legislador el "supuesto" criterio normativo vigente, es decir aquel manifestado en el D.S. 950 de 1928, que estableció un listado taxativo de las obligaciones impagas de carácter comercial que podían ser publicadas por el Boletín Comercial de la Cámara de Comercio de Santiago (el "Boletín Comercial")²⁹. Cabe decir supuesto, porque en verdad la propia Constitución Política (art. 19 N°24) y jurisprudencia³⁰ habían ya consagrado la libre iniciativa económica para la actividad de publicar información comercial, y por lo tanto el criterio normativo vigente era en realidad el de libertad amplia y no de una nómina cerrada establecida por la autoridad administrativa. Sin perjuicio de que era perfectamente posible que convivieran el Boletín Comercial, como una base de datos que comunicaba sólo una determinada clase de obligaciones comerciales, con otras bases de datos, también privadas, que podían comunicar todo tipo de informaciones comerciales.

De esta forma, se acogió el criterio de que la información comercial actualmente publicada en el Boletín Comercial era suficiente, añadiendo sólo aquella correspondiente a las sociedades administradoras de créditos otorgados para compras en casas comerciales (art. 17). Dicho sistema de información restringida debía imponerse por sobre el sistema de libertad empresarial y del derecho de información contemplado en la Constitución, y para el caso de necesidades futuras de información, se introduce el recurso al acto

²⁸ Id.

²⁹ La nómina de obligaciones publicables, contemplada en dicho decreto, se ha ido ampliando mediante la dictación posterior de otros decretos modificatorios.

³⁰ Véase el Capítulo II de este trabajo.

específico de la autoridad administrativa³¹ que, como se señaló, se ha utilizado bajo la vigencia del D.S. 950 (art. 17).

Podría argumentarse que una norma como la contemplada en la ley, si bien no se fundamenta en una protección razonable del derecho a la intimidad, pudiera ser útil para proteger el derecho a la honra o buen nombre comercial de los titulares de los datos; pero parece, por el contrario, que 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*. En cierta forma, el fundamento esgrimido para la inclusión —en la nómina taxativa de obligaciones comunicables— de las obligaciones correspondientes a las sociedades administradoras de créditos otorgados para compras en casas comerciales, esto es, su importancia en términos de volumen crediticio para la actividad económica actual³², deja de manifiesto la falta de lógica normativa y lo difícil que puede resultar justificar la construcción de los datos comerciales como una categoría especial de datos personales.

2. LOS CONCEPTOS DE TRATAMIENTO Y COMUNICACIÓN DE DATOS

Resulta interesante destacar la diferencia de género a especie, desde un punto de vista normativo, que existe entre tratamiento y comunicación de datos personales. Puesto que, por ejemplo, la ley permite el tratamiento de los datos que figuren en fuentes accesibles al público, cuando sean de carácter comercial —sin distinción— o cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios (art. 4°). En cambio, la ley sólo permite la comunicación de los datos comerciales —sea cual fuere su origen— que figuren en la nómina legal o en el acto de la autoridad administrativa (art. 17). Así, no es posible comunicar datos que sí han podido ser tratados.

Por otra parte, datos que durante un tiempo pudieron ser legítimamente comunicados, después de cumplidas ciertas condiciones o transcurrido un determinado plazo, sólo pueden ser mantenidos

³¹ No nos parece razonable, y puede dar lugar a un ejercicio de facultades arbitrario, el hecho de tener que estar recurriendo permanentemente a la autoridad para que ésta permita a las bases de datos comunicar información de contenido económico, financiero, bancario o comercial, sobre la cual puede existir una importante demanda insatisfecha. Este sistema nunca será tan dinámico como lo son las necesidades de una economía fundada en los pilares que contempla nuestra Carta Fundamental.

³² Boletín 896-07.

en los registros del banco de datos respectivo, pero no ser comunicados, es decir, el tratamiento se restringe y la comunicación se elimina. Ella sólo se mantiene para los Tribunales de Justicia. En todo caso, éstos sólo pueden requerirla con motivo de juicios pendientes (art. 17), no habiendo precisado la ley —como sí lo ha hecho en materia, por ejemplo, de secreto bancario (art. 154 de la Ley General de Bancos)— que el titular de los datos debe tener la calidad de parte en el respectivo proceso judicial.

3. LA RELACIÓN ENTRE LOS PRINCIPIOS GENERALES DE LA LEY Y AQUELLOS PARTICULARES

No resulta fácil armonizar el principio general relativo a los datos comerciales contenido en el artículo 4° de la ley con el tratamiento que el Título III, en especial el artículo 17°, da a esa misma clase de datos personales.

Después de leer la norma legal y revisar la historia de su tramitación queda la impresión que en el artículo 4° se hallaba el principio general de la moción parlamentaria, en lo relativo al tratamiento de los datos personales de carácter comercial, el cual fue invertido por completo en el artículo 17° introducido por la Comisión Mixta. El principio general era la libertad de tratamiento cuando los datos comerciales provenían de fuentes accesibles al público, en cambio, la norma particular establece un principio distinto, sólo puede publicarse la información cuando se cumplan los siguientes requisitos copulativos:

- i) debe tratarse de obligaciones incumplidas;
- ii) ellas deben ser de carácter económico, financiero, bancario o comercial, y
- iii) ellas deben constar en ciertos documentos³³, o versar sobre el incumplimiento de obligaciones con cierto tipo

³³ Letras de cambio, pagarés y cheques protestados. Se debe destacar que tales obligaciones se diferencian de aquellos casos contemplados en el artículo 1° N° 1° del D.S. 950 de 1928 que contempla la publicación de letras protestadas por los notarios por falta de aceptación o pago; del artículo 1° N° 6°, de la misma norma legal, relativa al protesto de letras y pagarés por parte de bancos y sociedades financieras por falta de pago cuando la firma del aceptante o suscriptor se encontrare autorizada ante notario; del Decreto N° 873 del Ministerio de Hacienda, D.O. de 22.10.77, relativo a la publicación de pagarés protestados por los notarios por falta de pago, y por último, el Decreto N° 1971 del Ministerio de Hacienda, D.O. de 13.04.45, relativo a la publicación en el caso de los cheques protestados, pero exclusivamente cuando la causal de protesto es la falta de fondos o por haber sido girados contra cuenta cerrada. En conclusión, la norma del artículo 17° de la ley es bastante más imprecisa que la normativa existente anteriormente.

de acreedores³⁴. Adicionalmente, se podrán comunicar aquellas obligaciones de dinero que determine el Presidente de la República, mediante decreto supremo, pero siempre que estén sustentadas en instrumentos de pago o de crédito válidamente emitidos y en las cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento (art. 17).

De esta forma, la norma particular alteró sustancialmente el principio general en esta materia, que era coincidente con el objetivo del proyecto, esto es, la protección de la vida privada. No estando, en nuestra opinión, en presencia de datos sensibles ni que afecten a la intimidad o la vida privada, se prohíbe la comunicación de informaciones que no reúnan los requisitos copulativos enunciados. Así, no podrán comunicarse obligaciones, aunque se encuentren incumplidas, cuyos acreedores sean empresas o entidades distintas de las consignadas en el artículo 17º, por ejemplo, empresas de *leasing* o *factoring*, de servicios de utilidad pública, o cualquier casa comercial que no haya organizado una administradora de crédito, o no cuenten con algunos de los instrumentos taxativamente requeridos por la Ley³⁵. Tampoco podrá comunicarse ninguna clase de información de este tipo cuando se trate de obligaciones vigentes o ya cumplidas³⁶.

4. LA ANALOGÍA ENTRE LOS DATOS PERSONALES COMERCIALES Y LOS RELATIVOS A SANCIONES PENALES O ADMINISTRATIVAS

Como expresamente se señaló en la Comisión³⁷, la prohibición de comunicar la información a que se refiere el artículo 17, después

³⁴ Mutuos hipotecarios y préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común y de sociedades administradoras de créditos para compras en casas comerciales.

³⁵ Parecen muy cuestionables, desde distintas perspectivas —tratamiento sistemático, lógica, dogmática, económica—, las discriminaciones introducidas por el artículo 17º de la ley.

³⁶ Una notable excepción a esta restricción pueden constituir los "sistemas de información comercial cerrados o privados" que hace posible el artículo 4º de la ley, o aquellos contemplados en otros cuerpos legales, por ejemplo, en el caso del sistema de información para bancos y sociedades financieras contemplado por el artículo 14 del D.F.L. N° 3 de 1997, texto refundido de la Ley General de Bancos.

³⁷ Boletín 896-07.

de transcurridos 7 años desde que la respectiva obligación se hizo exigible o 3 años después de extinguida una obligación, significa el término de los denominados “archivos históricos” una vez cumplidos dichos plazos. La norma siguió la misma lógica del artículo 21° de la Ley –relativo al tratamiento de los datos personales sobre delitos, infracciones administrativas o faltas disciplinarias por organismos públicos–, “en cuanto a que la información desfavorable de una persona sólo continúe proporcionándose en la medida en que haya interés, y no lo habrá si la obligación –o la sanción, en su caso– ha sido cumplida y ha transcurrido un plazo prudencial desde ese hecho; o si ya no es posible perseguir judicialmente la responsabilidad por haber prescrito la acción. La prohibición de suministrar dicha información, en ese sentido –se indicó–, permitirá al titular del dato volver a actuar con la necesaria normalidad”³⁸.

Se puede entonces señalar que esta homologación de información respecto de la conducta comercial de una persona con su posible prontuario criminal supone de cierta forma que ambos tipos de información, una vez transcurrido un cierto plazo desde que cesa el interés jurídico, generan tan poco beneficio a terceros o a la sociedad que la salvaguarda del derecho a la información ya no justifica afectar el derecho al honor. Después de transcurrido cierto tiempo, se invierte el orden de prelación en la protección legal, haciéndose prevalecer el derecho al honor frente al derecho a la información.

V. ALGUNOS PROBLEMAS Y POSIBLES SOLUCIONES

Por último, es conveniente tratar brevemente dos materias que pudieran ser fuentes de algunos problemas jurídico-económicos y sus posibles soluciones:

1. La restricción a la oferta de información comercial y el caso de las sociedades administradoras de crédito de las casas comerciales, y
2. Los sistemas de información comercial cerrados o privados.

³⁸ Id. Intervención del H. senador señor Viera-Gallo.

1. LA RESTRICCIÓN A LA OFERTA DE INFORMACIÓN COMERCIAL
Y EL CASO DE LAS SOCIEDADES ADMINISTRADORAS DE
CRÉDITO DE LAS CASAS COMERCIALES

Como se ha señalado, el artículo 17° de la ley contempló un sistema en que la única información que se puede publicar es aquella que se contempla en la norma legal, la que coincide —salvo en lo relativo a ciertos protestos de letras de cambio, pagarés y cheques³⁹— con lo preceptuado en el Decreto Supremo de Hacienda N° 950 de 1928, y que fue calificada por representantes de la propia Cámara como la información “suficiente” para el desarrollo de la actividad económica, con la única excepción de la información proveniente de las sociedades administradoras de crédito de las casas comerciales, las que, por la importancia que han adquirido en el mercado crediticio, deberían razonablemente ser incluidas. La propia ley en su artículo 3° transitorio ha ratificado la vigencia del referido decreto, elevándolo tácitamente a la categoría legal para estos fines, en todo aquello en que su contenido no contravenga la nueva ley.

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 del mercado. Cualquier otro competidor debe recurrir a dicha fuente matriz o acordar individualmente con cada productor de la información para obtener la misma información que obligatoriamente le es proporcionada a 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 ésta será la fuente primaria de información comercial para todo el mercado⁴⁰. Además, el hecho de aclarar la información en el Boletín

³⁹ Véase nota 33.

⁴⁰ Resulta interesante destacar que, con posterioridad a la preparación de este trabajo, se ha producido un intenso debate jurídico y comercial respecto de los distintos roles, derechos y obligaciones del Boletín Comercial en relación a otras bases de datos privadas.

Comercial implicará de inmediato que los demás bancos de datos en que se encuentre registrada la misma información deberán proceder automáticamente a modificarla⁴¹. Así lo dispone el inciso 3° del artículo 19 de la ley, para todos aquellos que hubieren efectuado el tratamiento de los datos provenientes o recolectados de la fuente accesible al público que fue objeto de la aclaración, la que en la mayoría de los casos será el Boletín Comercial.

Todo lo anterior implica que, de alguna forma, la competencia entre las distintas bases de datos comerciales ahora tendrá como principal objetivo lograr obtener como clientes fuentes de información a las sociedades administradoras de crédito de las casas comerciales, las que —como se ha visto— no se encuentran obligadas a proporcionar su información al Boletín Comercial. La fuerza de la competencia entre el Boletín Comercial, por la posición de privilegio en que lo colocó el legislador, y las restantes bases de datos es una cuestión que está por verse y que probablemente dará lugar a permanentes conflictos jurídicos⁴².

Por otra parte, y en relación con todos aquellos acreedores que quedaron excluidos de la posibilidad de publicar las obligaciones incumplidas de sus deudores, y como lo sugirieron los propios representantes de la Cámara de Comercio de Santiago ante la Comisión Mixta⁴³, se verán obligados —siempre que sus acreencias cumplan con las exigencias contenidas en el inciso segundo del artículo 17^o⁴⁴— a recurrir a la autoridad administrativa, siguiendo el camino ya recorrido por muchas instituciones en relación al texto del Decreto Supremo N° 950 de 1928, para que las incorpore dentro de la nómina de las “privilegiadas”. Seguramente se buscará, por algunos, que el mismo decreto modifique el D.S. N° 950 de modo de obligar a estos “favorecidos” a proporcionar su información al Bole-

⁴¹ Esta materia, por sus importantes consecuencias económicas, también ha sido objeto de debate posterior. Uno de los puntos que más se discuten es el derecho del acreedor o del deudor de solicitar la aclaración, en los casos previstos por la ley, en cualquier base de datos en que se encuentra registrada su deuda, en contraposición a la obligación a utilizar sólo el Boletín Comercial para tal efecto, y la posterior obligación de todas las otras bases de datos —incluido el Boletín Comercial—, una vez efectuada la aclaración respectiva, de proceder a su vez a modificar su respectiva información respecto del deudor.

⁴² Esos conflictos, como se ha señalado, ya han comenzado y hasta este momento no han llegado a instancias judiciales o administrativas (comisiones antimonopolios).

⁴³ Boletín 896-07.

⁴⁴ Entre ellas, la exigencia de los documentos hayan sido válidamente emitidos parece un requisito anómalo puesto que presumiéndose en general la validez de los actos jurídicos, modifica el peso de la prueba, lo que puede hacer a la norma inoperante.

tín Comercial. No nos parece que esta vía de concesiones de la autoridad, para la producción de un bien tan importante para el desenvolvimiento de una economía de mercado, como es la información comercial, haya sido la más adecuada a seguir.

2. LOS SISTEMAS DE INFORMACIÓN COMERCIAL CERRADOS O PRIVADOS

Por último, corresponde referirse a la norma contemplada en el último inciso del artículo 4° de la ley, el que en nuestra opinión podría adquirir una importancia relevante, a la luz de las restricciones ya mencionadas impuestas por el artículo 17°.

Esta norma es una de las excepciones en que no se requiere autorización del titular de los datos para el tratamiento —lo que sabemos en principio incluye su comunicación— “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” (art. 4°).

Como ya se señaló, en la Comisión Mixta⁴⁵ la Asociación de Aseguradores A.G. hizo presente la necesidad de contemplar una norma como la que en definitiva se incorporó, puesto que ella permitiría en relación a su actividad alcanzar, entre otros, los siguientes fines: una mejor detección de posibles fraudes, determinar mejor la naturaleza y probabilidad de ocurrencia de los riesgos, una adecuada formulación de políticas de cobro de primas, “ya que, de esa manera, se pueden cobrar primas más bajas a aquellos asegurados que presentan historiales de siniestralidad más baja y, a la vez, cobrar primas más altas a quienes acusan una siniestralidad mayor. Es decir, permitiría —en palabras de la propia Asociación— una tarificación más equitativa, ya que de otra manera la siniestralidad alta en que incurrir algunas personas simplemente pasaría a formar parte de la siniestralidad general y con ello se incrementaría la totalidad de las primas, en lugar de que éstas sean recargadas solamente a aquellas que acusan un nivel más alto de siniestros”⁴⁶. Además, se indicó, dicha información que produce el mercado asegurador era utilizada exclusivamente por las aseguradoras y la

⁴⁵ Boletín 896-07.

⁴⁶ Id. Intervención de la Asociación de Aseguradores de Chile A.G.

que pudiera difundirse se hacía sólo bajo la forma de información estadística, sin identificación de los titulares, como en definitiva lo permitió la ley.

¿Por qué nos hemos referido en extenso a dicha presentación ante la Comisión Mixta? Porque estimamos que las razones de fondo allí esgrimidas para la justificación de la norma y el impacto que ella causa en los titulares de los respectivos datos son exactamente las mismas que existen para el tratamiento de la información comercial. Su conocimiento por los proveedores de crédito —en sus diversas especies— también es fundamental para una mejor detección de posibles fraudes, determinar mejor la naturaleza y probabilidad de ocurrencia de los riesgos, una adecuada formulación de políticas de cobro y una tarificación más equitativa. ¿Entonces qué deben hacer estos proveedores de crédito para poder hacer uso de la misma oportunidad que la ley les otorga a otros?; nos parece que una alternativa posible es organizarse de modo que la información comercial fluya entre ellos de la forma que lo permite la norma, esto es, entre asociados de las personas jurídicas privadas que pueden estar constituidas, entre otros, para tales fines y también entre las distintas entidades relacionadas y afiliadas.

Este sistema de información cerrado, entre los miembros de una determinada categoría, es de hecho el sistema que actualmente existe entre los bancos y las sociedades financieras, los cuales — como se sabe— se encuentran obligados a proporcionar a la Superintendencia respectiva la nómina de los deudores de las instituciones financieras, los saldos de sus obligaciones y las garantías que hayan constituido. Esta información está a disposición para su uso por todas las instituciones financieras⁴⁷.

Podría argumentarse que, en el caso de la información de carácter comercial, el artículo 17° de la ley resulta especial en relación al inciso final del artículo 4° y por lo tanto excluiría la aplicación de una norma general como sería esta última. No parece que sea ésa una interpretación correcta de la ley, entre otras, por las siguientes razones:

- i) porque ambas normas pueden ser aplicadas respecto de la información comercial sin un conflicto real, así el artículo 4° permitirá la difusión de la información entre los

⁴⁷ Artículo 14 del D.F.L. N° 3 de 1997, texto refundido de la Ley General de Bancos.

- asociados, y el artículo 17 la restringirá respecto del público en general;
- ii) porque el propio texto del inciso final del artículo 4° se refiere a “datos personales” sin calificarlos, como sí se hace en el inciso anterior, lo que implicaría que la norma es de general aplicación a todo tipo de datos personales excepto los sensibles –los que, según se ha visto, también tienen su propia norma de comunicación para los prestadores de servicios (art. 10)–;
 - iii) porque una interpretación de este tipo permitiría conciliar en mucho mejor forma la protección del derecho al honor con el derecho a la información, al evitar la propagación al público en general de la información respectiva, y
 - iv) porque al configurarse una asociación de usuarios de la información comercial se fomenta la autorregulación y se facilita la determinación de posibles responsables, lo que implica mayor seriedad y garantiza información más fidedigna, cuya inexistencia habría justificado legalmente la consagración del sistema de censura previa contemplado en el artículo 17°.

Es decir, nos parece que la norma en cuestión permite utilizar el derecho de asociación como una forma de incrementar el uso de información comercial entre los distintos asociados y de esta forma incrementar su producción con el consiguiente beneficio para las partes y la economía como un todo.

VI. CONCLUSIONES

Concluyendo, cabe puntualizar algunas cuestiones que nos parecen básicas:

1. La ley no recogió en buena forma la justa aspiración de un equilibrio razonable entre el derecho a la intimidad y a la honra y la necesidad de información comercial, con el importante rol que ésta tiene en el desarrollo de una economía de mercado;

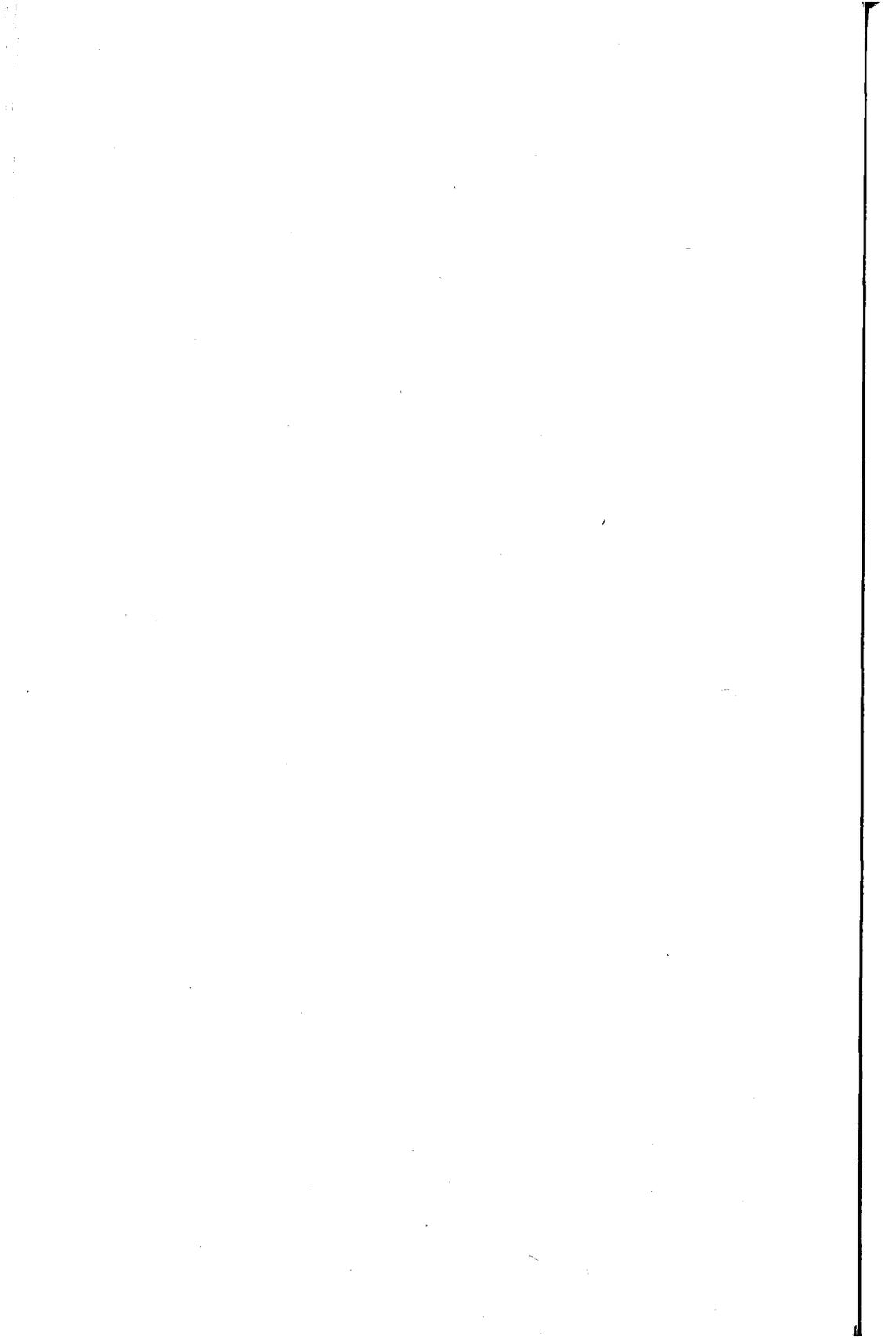
2. Pudo haber sido más adecuado –en lugar de contemplar una nómina taxativa de información comercial comunicable– contemplar un sistema de libertad de información, pero con algunos con-

trapesos que permitieran respetar los legítimos intereses de los titulares de los datos;

3. En este último aspecto, el derecho de asociación entre los acreedores puede jugar un importante rol en la producción y comunicación de aquella información comercial que quedó excluida del listado taxativo contemplado por el artículo 17° de la ley;

4. El establecimiento de determinados plazos para ser “borrado” de los “registros históricos” puede significar un apoyo al ejercicio de la actividad empresarial, con los riesgos y beneficios que ella impone, como también a la actividad del consumo, con el rol que ella juega en nuestra economía. Ambas “rehabilitaciones” nos parece que pueden aportar más beneficios que costos, y

5. Por último, resulta lamentable que la incorporación en el último momento legislativo de una norma de la importancia del artículo 17° haya significado —como se ha señalado— que se tomaran importantes opciones normativas sin considerar suficientemente la experiencia comparada y la propia jurisprudencia nacional y se haya caído en contradicciones entre dicha norma y los principios generales contemplados en la misma ley. Ello, sin duda, será terreno fértil para la discusión jurídica y la menor eficacia de la protección de derechos constitucionales de importancia fundamental en una sociedad de la información.



LA LEY CHILENA DE PROTECCIÓN DE DATOS PERSONALES. UNA VISIÓN CRÍTICA DESDE EL PUNTO DE VISTA DE LOS INTERESES PROTEGIDOS

RENATO JIJENA LEIVA

*Profesor de Derecho Informático y del Diplomado
en E-Business de la Universidad de Chile*

I. INTRODUCCIÓN

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

Para un adecuado análisis de la ley en comento se propone el siguiente desarrollo expositivo:

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

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

En el Capítulo IV, recogiendo los elementos previamente expuestos, se revisa brevemente cuál fue la tramitación parlamentaria

de la ley aprobada y cuál es el contenido y los alcances de los artículos que la conforman, para cerrar los comentarios formulando algunas observaciones generales a la ley.

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

1. GENERALIDADES

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

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

Un dato es personal o nominativo cuando permite identificar cualquiera característica de una persona para relacionarse en sociedad, por ejemplo al consignarse en una guía de teléfonos datos generales, o cuando son de mayor importancia o sensibilidad como ocurre con la filiación política, el credo religioso que se profesa, los antecedentes laborales, la situación de salud, la mayor o menor riqueza, las operaciones comerciales que se realizan, las acciones en empresas que se poseen, los depósitos en cuenta corriente o a plazo, los impuestos pagados, etc.

2. EL PROBLEMA DE FONDO SE ORIGINA POR UN CONFLICTO ENTRE DOS INTERESES RELEVANTES

Por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc.

Por el otro, un interés —también muy legítimo— que poseen los gobiernos y los particulares para acceder a cierta información: los

Estados para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quiénes tienen SIDA al momento de fijar políticas de salud, y los particulares, generalmente constituidos en empresas de servicios o entidades gremiales, que para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial.

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

La interrogante a dilucidar o la hipótesis de trabajo, en consecuencia, puede ser la siguiente: ¿cómo conciliar el Derecho a la Información con el Derecho a la Intimidad?; ¿cómo equilibrar por un lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad? Se trata de una cuestión importante por cierto, no de meras disquisiciones teóricas o doctrinarias, porque si bien el orden público social y económico de una Nación requiere que tanto el Estado como los particulares manejen determinados datos personales, sea para fijar políticas de salud o para evitar la morosidad comercial, esto no puede traducirse, al extremo, en abusos contra las personas. Así ha ocurrido con la información comercial o sobre los antecedentes patrimoniales de los chilenos, que en base a inexistentes argumentos legales o erradas interpretaciones constitucionales hasta antes de la ley era procesada y comercializada sin límite alguno¹ y hoy en día, al tenor de la nueva ley aprobada que se informa, se hace con límites mínimos o meramente formales.

La respuesta doctrinaria ha sido la formulación de un nuevo concepto del Derecho a la Intimidad, que surge frente a la llamada o reclamada *libertad informática* o de procesamiento de datos personales-nominativos, que deja de lado el enfoque individualista

¹ Con ocasión de la interposición de recursos de protección en contra de la empresa Dicom S.A. se ha argumentado, sobre la base de interpretar las Actas de la Constitución de 1980 pero sin fundamento serio, que la Carta Fundamental distinguiría entre un *patrimonio moral* y un *patrimonio económico* de las personas; por ende —lo que es un absurdo y una falacia, porque el debate nunca fue abordado por el Constituyente y porque entre los años 1977 y 1979 el problema del procesamiento computacional de datos personales no existía—, ciertos datos que conformarían el primero serían reservados y el segundo comprendería toda la información comercial/nominativa que sería pública, tendiendo la sociedad derecho a conocerla y Dicom a recopilarla, procesarla, cruzarla y comercializarla.

o negativo con que fue concebido para plantearse desde una perspectiva socializadora y positiva (ya no es "el derecho a ser dejado a solas"), y que se concibe como la posibilidad de que los ciudadanos titulares y propietarios de los datos que les conciernan controlen el uso y el eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente.

3. SOLUCIÓN AL PROBLEMA DE DETERMINAR QUÉ ANTECEDENTES FORMAN PARTE DE LA LLAMADA "ESFERA PRIVADA" Y CUÁLES DE LA "ESFERA PÚBLICA" DE LAS PERSONAS

Los órganos estatales y las empresas comerciales que a partir de nuestro número de identificación nacional procesan información personal se han preocupado de aclarar que ellos sólo estarían manejando o procesando ciertos "datos públicos". Esto es delicado, porque el límite entre la esfera privada y la esfera social o pública de una persona no se ha establecido legalmente con claridad, y porque el problema de los cotidianos atentados contra la vida privada, la igualdad laboral, la igualdad ante la ley y la libre iniciativa en materia económica —para nombrar algunas garantías fundamentales afectadas— surge cuando se cruzan computacionalmente y con toda facilidad antecedentes personales y se elaboran perfiles.

En la medida que un particular consienta o una norma legal establezca que ciertos datos o antecedentes personales sean susceptibles de conocerse², éstos pasarán a formar parte de una esfera social o pública porque lo vincularán con la sociedad.

En el caso contrario, esto es, si cada titular de los datos que lo individualizan opta por mantenerlos reservados o no existe una ley que por razones de orden público permita expresamente conocerlos³, tales antecedentes, que les pertenecen⁴, serán parte de una

² Pensemos en los siguientes datos: número de teléfono, profesión, filiación política, origen étnico; situación laboral, cotizaciones previsionales, monto de impuestos declarados; créditos bancarios obtenidos, viajes realizados, valores transados en la Bolsa, participaciones en sociedades; etcétera.

³ Tal es el caso del prontuario o registro de condenas, de la base de datos del Servicio de Registro Electoral, del Boletín Comercial de la Cámara de Comercio de Santiago, etcétera.

⁴ A propósito de los datos patrimoniales, desde 1929 a la fecha la Superintendencia de Bancos ha sostenido que uno de los atributos del dominio lo constituye la facultad exclusiva del dueño para permitir o impedir a terceros que se impongan o no de sus negocios.

esfera íntima o reservada que no puede ser atisbada, procesada o conocida por particulares, por empresas que quieran comercializarlos e incluso por órganos estatales. Dichos datos en Chile están protegidos por la esfera íntima que consagra la garantía del artículo 19 N°4 de la Constitución.

4. DERECHO DE ACCESO O *HÁBEAS DATA*

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

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

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

5. ¿CÓMO LOGRAN LAS LEYES DE PROTECCIÓN DE DATOS, VIGENTES DESDE HACE 20 AÑOS EN EL DERECHO COMPARADO, EL EQUILIBRIO DE LOS INTERESES INVOLUCRADOS?

Básicamente de la siguiente forma: no se niega la posibilidad del procesamiento o tratamiento de datos, pero se consagran facultades de acceder, corregir, actualizar o eliminar datos para los titulares de los mismos (enmarcadas en el denominado *Hábeas Data*); se establecen mayores limitaciones para el procesamiento cuando los da-

tos son de especial relevancia como los llamados “sensibles” o “personalísimos” (vida sexual, salud, raza, credo religioso, filiación política, etc.); se regula separadamente el procesamiento que realice un órgano público, una persona natural o una persona jurídica, estableciendo diferentes requisitos de constitución; se regulan acabadamente las obligaciones y prohibiciones del responsable de un sistema; se radica la operatividad de todas las normas en un órgano autónomo de control y fiscalización, “a priori” –autorizando a procesar y fijando los requisitos para hacerlo– y “a posteriori” –conociendo de los reclamos y sancionando–, y se configuran sanciones administrativas y penales para el caso que las normas de la ley no se cumplan.

Todas las *Data Protection Act* tienen la siguiente estructura, a saber, una parte dogmática, una parte orgánica, una parte procedimental y una parte sancionatoria o represiva. Revisemos brevemente esta estructura:

Parte Dogmática: Comprende los conceptos esenciales, principios inspiradores, ámbito de aplicación, especies o categorías de datos protegidos, consagración del Derecho de Acceso o *Hábeas Data* y de sus garantías derivadas, derechos, obligaciones, restricciones y prohibiciones para los responsables de los sistemas de tratamiento de datos personales, etcétera.

Parte Orgánica: Se refiere a la autoridad *ad hoc* independiente, técnicamente competente y con facultades normativas, de control y fiscalización a priori y a posteriori, y sancionatorias sobre los responsables de los bancos de datos personales; a la existencia de un registro público de los responsables y los bancos de datos, etcétera.

Aspectos Procedimentales: Se regulan instancias de reclamos de rápida y breve tramitación y fallo ante el órgano *ad hoc* (agotamiento previo de la vía administrativa); la posibilidad de interponer recursos posteriores ante los tribunales superiores de justicia, etcétera.

Parte Represiva o Sancionatoria: Incluye la cancelación de la autorización de funcionamiento y eliminación del registro, multas, tipificación de delitos, etc.

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

1. PROCESAMIENTO DE DATOS PERSONALES EN LOS SECTORES PÚBLICO Y PRIVADO

Los cotidianos atentados contra la privacidad de los chilenos, tanto en cuanto datos personales o nominativos tratados mediante sistemas informáticos, desde hace bastante tiempo vienen cometiéndose por órganos estatales y por empresas comerciales, en particular por estas últimas. Uno de los temas que subyace en este debate es la necesidad de regular un ámbito de prestación de servicios comerciales que puede afectar derechos de las personas tales como la vida privada, el acceso al crédito, la libertad de trabajo, la libre iniciativa en materia económica y la igualdad ante la ley.

2. LA PROPIEDAD DE LOS DATOS

También en Chile varias multitiendas comerciales exigen, al momento de otorgar créditos y facilidades de pago, una serie de datos que posteriormente almacenan computacionalmente; pública y gremialmente han vindicado la propiedad de dicha información. Una empresa chilena que ofrece productos de bases de datos en Internet (v.gr. guías de empresas) advierte en su página WEB que está otorgando el derecho de acceder a sus bases exclusivamente a modo de consulta, que bajo ninguna circunstancia puede arrendarse o venderse parte o toda la información recopilada y ofrecida, y que el contenido de las bases de datos es de su propiedad y está protegido por el derecho de autor.

Estas afirmaciones son, a nuestro juicio, erradas, toda vez que son cosas muy distintas *"el continente"* o la estructura de la base o banco de datos que *"el contenido"* o la información almacenada en el mismo.

Las normas internacionales de mayor importancia que aluden al tema, a saber, el acuerdo TRIP del GATT y la OMC adoptado en 1994 en Marrakech sobre aspectos de la propiedad intelectual relacionados con el comercio (Anexo 1C, artículo 10°), la Directiva de la Unión Europea 96/9/CE de 1996 y el Tratado sobre Derecho de Autor de la OMPI adoptado a fines de 1996 en Ginebra (artículo 5°)

establecen claramente que la Propiedad Intelectual ampara a las compilaciones de datos cuya selección o disposición de contenidos sean creaciones originales y señalan expresamente que dicha protección autoral no abarca a la información compilada o "a los datos en sí mismos".

Las empresas aludidas sólo pueden considerarse propietarias intelectuales del diseño y estructura original del fichero computacional, mas por el hecho de recopilar antecedentes sobre personas naturales y jurídicas, procesarlos, seleccionarlos, organizarlos o almacenarlos no se transforman —porque no existe título ni modo de adquirir alguno— en dueñas de la información nominativa que individualiza a otras personas, de manera tal que posteriormente puedan comercializarla libremente (sobre todo cruzada o en forma de "perfiles"). Incluso más: el carácter de depositarias o tenedoras de datos personales les impone obligaciones de confidencialidad y reserva, tan importantes como aquellas que emanan del secreto estadístico o del secreto bancario.

3. LOS DATOS PERSONALES-PATRIMONIALES O SOBRE SOLVENCIA PATRIMONIAL

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

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

Una distinción es esencial en materia de datos personales-patrimoniales, a saber, es que éstos pueden ser "*positivos*" o "*negativos*". Los primeros se refieren a aquellos antecedentes que dan cuenta de la composición del patrimonio de una persona, de cuán-

to posee, de cuánto gasta, de los créditos abiertos a su nombre, de su capacidad crediticia, etcétera. Los segundos son los que dan cuenta de conductas comerciales o financieras irregulares, por cuanto corresponden al incumplimiento de obligaciones previamente pactadas. Es del caso indicar que la regulación constitucional, legal y reglamentaria de ambos debe ser analizada desde distintas perspectivas⁵.

IV. ANÁLISIS DE LA LEY APROBADA

1. ESTRUCTURA Y CONTENIDO O IDEAS MATRICES DE LA LEY

La ley consta de un Título Preliminar sobre Disposiciones Generales (artículos 1º, 2º y 3º); de un Título I sobre la Utilización de Datos Personales (artículos 4º al 11º); de un Título II sobre Derechos de los Titulares de Datos (artículos 12º a 16º); de un Título III acerca de la Utilización de Datos Personales relativos a Obligaciones de Carácter Económico, Financiero, Bancario o Comercial (artículos 17º a 19º); de un Título IV sobre Tratamiento de Datos por Organismos Públicos (artículos 20º, 21º y 22º); de un Título V acerca de la Responsabilidad por las Infracciones a esta Ley (artículo 23º); de un Título Final que modifica el Código Sanitario (artículo 24º), y de tres disposiciones transitorias.

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

La regla general formalmente declarada por el texto legal es que dicho "*tratamiento de datos personales*" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "*fuentes de acceso público*" (por lo cual no se requiere de autorización para su tratamiento) y se consagran importantes

⁵ Téngase presente lo que establece, por ejemplo, el artículo 28 de la Lortad de España, relativo a la prestación de servicios de *información sobre solvencia patrimonial y crédito*. En él se distinguen dos supuestos claramente diferenciados de información, a saber, el que hace referencia a las posibilidades económicas y financieras de una persona natural y los datos relativos al incumplimiento de obligaciones dinerarias.

y amplias excepciones sobre todo en materia de datos "*personales-patrimoniales*", lo cual transforma a la regla general en una mera declaración de principios.

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

2. ÁMBITO DE APLICACIÓN

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

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

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

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

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

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

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

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

2.2 Ámbito de aplicación de la ley desde la perspectiva de los “Responsables de las Bases de Datos”

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

Todas las leyes de protección de datos en el Derecho Comparado establecen una clara diferenciación entre lo que son las bases de datos *públicas* y las *privadas*, en atención a la naturaleza de la entidad que las administra y no, como lo hace la ley chilena, en consideración a la fuente de la información o al tipo de datos procesados.

2.2.1. El artículo 2° letra k) define lo que son los Organismos Públicos, entendiendo por tales a “las autoridades, órganos del Esta-

do y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado”.

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

Para efectos de este informe cabe indicar que el artículo 22 contempla la obligación de que sea el Servicio de Registro Civil el ente que llevará un Registro Público de Bancos de Datos, pero sólo en relación a entes estatales y excluyendo de la obligación de registro a las empresas particulares. Esta disposición, fruto de una indicación presentada por el Ejecutivo durante el debate en Comisión Mixta ya que se trata de una materia de iniciativa exclusiva del Presidente, es de difícil comprensión, porque en sí no lleva envuelta el establecer una instancia o grado de fiscalización alguno, que es la razón de ser en las leyes de protección de datos de la existencia de órganos *ad hoc*⁶. ¿Cuáles son las sanciones a aplicar al órgano público que no se registre?; ¿puede el Servicio de Registro Civil realizar algún control al efecto y con qué facultades, si en Derecho Público sólo puede hacerse aquello que esté expresamente permitido?

Nunca se entendió la importancia de que la ley contemplara un órgano de fiscalización y la existencia de un registro *ad hoc*. Inicialmente no se abordó el tema bajo el débil argumento de “no querer ser burocráticos”; posteriormente se propuso que fuera la Contraloría General de la República⁷; luego se estableció (en el proyecto aprobado en el Senado) que sería un organismo público el encargado de llevar un registro de los bancos de datos tanto públicos como privados; la solución final elaborada en la Comisión Mixta, para hacer el sistema aún menos restrictivo para las empresas dedicadas al procesamiento de información, es insuficiente, porque ni siquiera incluye la obligación de registro para empresas o personas privadas.

⁶ Para entender la importancia y la operatividad práctica del tema, véase en Internet la dirección www.ag-protecciondatos.es/regis.html, que conecta con el Registro General de Protección de Datos existente desde 1992 en España.

⁷ En un informe presentado al Senado en mayo de 1998 reparamos esta iniciativa por inconstitucional, lo que fue acogido, según consta en las páginas 36 y 37 del informe final de la Comisión de Constitución, Legislación y Justicia del Senado.

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

3. NECESARIAS DISTINCIONES ACERCA DE LAS CATEGORÍAS DE DATOS

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

4. BREVES COMENTARIOS A LAS DEFINICIONES

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

Respecto de los datos se define cuando son "caducos"⁸, "estadísticos"⁹, "de carácter personal"¹⁰ o personal "sensible"¹¹.

Respecto de las actividades de las que pueden ser objeto los datos personales, el término más amplio que se define es "tratamiento de datos"¹², y derivados de éste, los conceptos de "almace-

⁸ Conforme lo establece la letra d) del artículo 2°, "dato caduco" es el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

⁹ Letra e): ...dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

¹⁰ Letra f): ...datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

¹¹ Son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

¹² Es cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

namiento”¹³, “bloqueo”¹⁴, “comunicación o transmisión”¹⁵, “eliminación o cancelación”¹⁶, “modificación”¹⁷ y “procedimiento de disociación”¹⁸.

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

Una novedad de la ley chilena es la incorporación en términos amplísimos, a diferencia de la ley española¹⁹, del concepto de “*fuentes accesibles al público*” en la letra i) del artículo 2º, las que legalmente han sido transformadas en la regla general.

Se definen amplia y ambiguamente como “los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado... a los solicitantes”.

La consecuencia práctica de esta norma es qué al ser los datos personales estimados por regla general como legalmente públicos, cualquiera puede procesarlos y comercializarlos porque el acceso a ellos está permitido por ley y sin restricciones, validándose el negocio del procesamiento y la venta de datos personales.

La primera cuestión a dilucidar es determinar cuáles son los registros que pueden ser considerados como “*de datos personales públicos o privados de acceso no restringido o reservado a los solicitantes*”, porque los que no detenten esta calidad, aquellos cuyo

¹³ Se entiende por tal la conservación o custodia de datos en un registro o banco de datos.

¹⁴ Consiste en la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

¹⁵ La comunicación o transmisión de datos consiste en dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

¹⁶ Es la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

¹⁷ Consiste en todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

¹⁸ Se entiende por tal a todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

¹⁹ El artículo 28 de la ley española regula las fuentes accesibles al público solamente con el objeto de establecer que de esta clase de registros o bancos de datos pueden obtenerse datos patrimoniales positivos, dejando fuera de su alcance a los demás datos, especialmente a los sensibles. En tal ley y las normas complementarias dictadas por la Agencia de Protección de Datos se entiende por “datos accesibles al público” aquellos que se encuentran a su disposición en forma general y no impedidos por cualquier norma limitativa (por ejemplo, datos de censos, anuarios, repertorios de jurisprudencia, archivos de prensa, guías telefónicas, etc.).

acceso no sea permitido sin restricciones o sea prohibido por ley, constituirán fuentes reservadas o no accesibles al público.

La ley no hace una categorización. No creemos que se trate de una cuestión meramente de hecho, sino que dicha determinación sólo podrá hacerse por los órganos jurisdiccionales, pero para casos concretos. No obstante, ya en Chile existen algunas fuentes de información que son de acceso restringido ya que existen leyes que previamente así lo han establecido al darle a los datos el carácter de reservados o confidenciales. Nos referimos a lo menos al secreto estadístico, al secreto tributario, al secreto bancario o al secreto de la filiación política. Al existir tales normas, son de acceso restringido; si no existieran (que es la regla general) serían de acceso permitido o fuentes públicas.

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

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

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

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

Cabe entonces concluir 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 nombradas—, o una norma o resolución administrativa o una cláusula contractual de confidencialidad establezcan expresamente lo contrario. Tal es el caso, por ejemplo, del Reglamento de la ley N° 19.653, sobre "Secreto o Reserva de los Actos y Documentos de la Administración del Estado" y que se conoce como la ley sobre la probidad administrativa y el acceso a la información del Estado establece en la letra b), numeral 5, del

artículo 8° que la declaración de secreto o reserva de los antecedentes privados procederá respecto de “los que contengan o se refieran a secretos industriales y comerciales, incluyendo a los procedimientos de fabricación, las informaciones económicas y financieras y las estrategias comerciales”.

5. ANÁLISIS DEL ARTÍCULO 4°²⁰

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

5.1 Regla general

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

²⁰ Artículo 4°. El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

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

La autorización debe constar por escrito.

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

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

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

Respecto a la *autorización* mediante la cual el titular de los datos personales consiente expresamente en el *tratamiento*²¹, señalan los incisos segundo, tercero y cuarto que tanto su otorgamiento como su revocación deben constar por escrito, que la revocación se produce sin efecto retroactivo, y que la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y de su posible "comunicación" al público. Como nada se dice, creemos que tal autorización podrá ser otorgada antes o después de iniciado el procesamiento, con lo cual tendría lugar la *ratificación*.

Fácil es concluir que dicha autorización se transformará en una amplia cláusula tipo, especialmente en los contratos de adhesión²².

5.2 Excepciones

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

Dichas situaciones de excepción son las siguientes:

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

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

²¹ Recuérdese que la letra o) del artículo 2º define como "tratamiento de datos" a "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".

²² Estas cláusulas no son ajenas al actual sistema financiero chileno. Así, por ejemplo, en las Condiciones Generales de la solicitud de productos de una Financiera se señala que el solicitante faculta a la entidad "para proporcionar a sus empresas relacionadas todos los datos referidos a mi individualización que he facilitado en la presente solicitud de crédito, tales como nombre y apellidos, estado civil, domicilio, profesión u oficio, Carnet de Identidad Nacional, Rut, y si fuera requerido para ello, lo faculto para informar a sus empresas relacionadas acerca de los depósitos y captaciones que mantengo y las obligaciones que he contratado...".

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

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

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

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

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

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

to al cual apuntará la campaña comercial o la venta de los productos.

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

La ley aprobada, a diferencia de toda la legislación extranjera, legaliza con mínimas limitaciones el *marketing* directo. El artículo 4° en comento establece como amplia excepción y perentoriamente que no se requiere autorización para el procesamiento de datos personales que provengan de fuentes públicas cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, lo que, sumado a las dos excepciones anteriores o perfilados con los datos a que ellas aluden, declara exento de autorización o control para el titular a un cúmulo demasiado grande de datos nominativos o personales²³.

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

Por otro lado, 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 que se refieren) puede

²³ Difícil tarea tendrán los congresistas que impulsaron la ley para explicar en el futuro la razón de que frente a una actividad esencial para las empresas de *marketing* directo y que sólo persigue fines de lucro o comerciales, inconstitucionalmente optaron por impedir que los chilenos "autodeterminen", autoricen y controlen el uso de sus antecedentes. Del mismo modo, se ha permitido legalmente que AFP, Isapre, multitiendas, universidades, asociaciones gremiales, órganos públicos, etc., puedan comercializar grandes cúmulos de información, siempre con la ignorancia y sin el consentimiento de los titulares y propietarios de los antecedentes que los individualizan.

oponerse —en nuestra opinión sin expresar causa alguna— a su uso “con fines de publicidad”. Habría que entender que el inciso quinto del artículo 4° prima por especialidad.

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

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

6. DATOS PERSONALES, ENCUESTAS, ESTUDIOS DE MERCADO Y PUBLICIDAD

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

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

Este derecho, al decir de un autor francés, refuerza el principio de que los titulares de los datos personales que les conciernen poseen un derecho de propiedad sobre los mismos, lo que se entiende si se tiene presente que se trata de información nominati-

va o personalísima referida a atributos de su personalidad, en concreto, a la intimidad o privacidad de las personas. Si bien es cierto hay quienes de la mano de nuestro Código Civil de 1855 sostienen que legalmente sólo podría vindicarse la titularidad del derecho real de dominio sobre "cosas"; que éstas sólo son "corporales" –tienen un ser real y pueden ser percibidas por los sentidos– o "incorporales" –meros derechos–, y que los "datos nominativos o personales" cuyo conjunto organizado constituye "información nominativa" y los derechos de la personalidad –por ende– no serían susceptibles de ser amparados por el instituto del dominio, ocurre que dichos autores por un lado desconocen o no acogen la teoría de la existencia de "derechos sobre derechos"²⁴ y, por otro, desconocen y no perciben el fenómeno de la desmaterialización provocada por las nuevas tecnologías como la informática, las telecomunicaciones y la telemática, en concreto, la existencia contemporánea de cosas intangibles e inmateriales como los programas y/o datos computacionales –el denominado "soporte lógico" de un sistema informático– y parten sus reflexiones de un supuesto obsoleto, reductivista, o limitado como es la clasificación o categorización de las cosas que hace el Código de Bello en meramente corporales o incorporales²⁵.

²⁴ Esta propiedad, dominio o titularidad dominical del conjunto de datos personales o nominativos, es decir, de la garantía de la intimidad de una persona, tanto en cuanto datos personales almacenados en un sistema computacional, que además debe entenderse como un derecho de la personalidad incorporado al patrimonio de una persona natural o incluso jurídica y del cual puede disponerse en forma exclusiva y excluyente, está protegida constitucionalmente por el artículo 19 N° 24 de la CPE. Es lo dicho por aquella vieja frase de la existencia de "derechos sobre derechos", o más concretamente, "de derechos reales de dominio sobre el derecho personalísimo de la intimidad registrada como antecedente o dato binario en una base o banco de datos computacionales. *A contrario sensu*, están los que sostienen que pasan a ser dueños de la información o titulares del derecho de propiedad sobre la información o "contenido" de una base de datos personales o nominativos, por el solo hecho de recopilarlos y sin haber solicitado previamente su autorización al titular o la persona a que ellos aluden e individualizan.

²⁵ La clasificación de las cosas en corporales e incorporales a que aluden los artículos 565 y 576 del Código Civil ha sido superada por la realidad del siglo XXI y debe ser reformulada.

A diferencia de lo que ocurre en el Derecho Comparado, el ordenamiento jurídico chileno define a los bienes o cosas y los clasifica, como se dijo, en corporales o incorporales.

Es forzoso concluir que esta clasificación no permite incluir al soporte lógico de un sistema computacional, sean "datos" o "programas computacionales", ya que ambos no son derechos reales o personales y por ende no pueden legalmente ser calificados en Chile como cosas incorporales. Menos puede pretenderse que datos y programas sean cosas corporales perceptibles lógicamente por los sentidos, ya que son impulsos electromagnéticos que se transmiten a través de circuitos electrónicos no perceptibles por los sentidos del hombre y que eventualmente se visualizan en una pantalla en el evento que el computador esté encendido.

7. LA RELEVANTE FIGURA DEL "RESPONSABLE DEL REGISTRO O BANCO DE DATOS PERSONALES"

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

El mismo artículo define lo que debe entenderse por "registro o banco de datos", a saber, "el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos".

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

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

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

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

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

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

Debe concluirse además que para el legislador chileno no son equivalentes los términos "cosas incorporales" y "cosas inmateriales e intangibles". Estas últimas serían todas aquellas entidades que no tengan una existencia física o corporal tradicional, que sólo puedan percibirse mental o intelectualmente, y que no consistan en meros derechos reales o personales.

Es por eso que la doctrina ya ha propuesto formular una nueva clasificación de los bienes o de las cosas. En un libro de octubre de 1995, titulado "*Las cosas incorporales en la doctrina y el derecho positivo*", y en que expresamente se alude a la categoría de "*cosas intelectuales o ideales*", luego de reconstruir intelectualmente el concepto de "cosa incorporal" para hacerlo equivalente o sinónimo a "derecho" en sentido subjetivo, y de criticar la tradicional dicotomía de cosas clasificadas en corporales e incorporales, el profesor Alejandro Guzmán Brito propone la existencia de una tercera categoría de bienes (por ende susceptibles de incorporarse al patrimonio y de ser amparadas por el derecho de propiedad) para aludir a cosas dotadas de autonomía conceptual.

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

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

8. EL *HÁBEAS DATA* O DERECHO DE ACCESO

Esta garantía esencial de toda ley de protección de datos y las facultades que de ella derivan, mismas que por su importancia en varios países tienen rango constitucional, están reguladas en los artículos 12°, 13°, 14° y 15° de la ley, que son los primeros del Título II sobre Derechos de los titulares de datos, y se ejercen precisamente ante quien aparezca como responsable del registro.

En síntesis, la ley establece inicialmente que toda persona tiene *derecho a exigir -a quien sea responsable de un registro banco de datos que se dedique en forma pública o privada al tratamiento de datos personales-, información* sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

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

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

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

El ejercicio de estas facultades no conlleva derecho a cobro por el responsable del registro, toda vez que se señala expresamente

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

Para el evento que los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada y si no fuese posible determinar las personas a quienes se les hayan comunicado, deberá publicarse un aviso que pueda ser de general conocimiento para quienes usen la información.

9. CONDICIONES PARA LA TRANSMISIÓN DE DATOS VÍA REDES ELECTRÓNICAS

El artículo 5° establece que, tratándose de datos que sean de acceso restringido o reservado²⁶, 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. Surge una pregunta: ¿quién calificará que el resguardo de los derechos es adecuado y que se adecua a los fines de quienes tienen acceso a la red?

En el supuesto de estar ya conectados en red, el responsable, frente a un requerimiento de datos personales, deberá dejar constancia de la individualización del requirente, del motivo y el propósito del requerimiento y del tipo de datos que se transmitan. Previamente deberá evaluar a su sólo arbitrio la admisibilidad del requerimiento, pero la *responsabilidad* por dicha petición —dice la ley— será de quien la haga.

²⁶ La ley establece que no se aplicarán las limitantes de este artículo cuando se transmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en tratados y convenios vigentes, ni cuando se trate de datos personales accesibles al público en general; es decir, y entendiéndose que éstos son la regla general, en la práctica no se aplicará nunca. Además que al efecto Chile no ha suscrito a la fecha tratado alguno.

10. INTEGRIDAD, IDONEIDAD, EXACTITUD Y FIDELIDAD
 DE LOS DATOS PERSONALES TRATADOS AUTOMATIZADA
 Y MANUALMENTE. ELIMINACIÓN, MODIFICACIÓN
 O BLOQUEO DE LOS MISMOS

El artículo 6º, extrañamente, repite varios de los conceptos también contenidos en el artículo 12. Ambos artículos debieron haberse refundido en uno solo. Repite la idea de que los datos personales pueden *eliminarse o cancelarse* cuando hayan sido almacenados sin fundamento legal o cuando estén caducos²⁷. Señala que deberán *modificarse* cuando sean errados, inexactos, equívocos o incompletos²⁸. Lo que es nuevo y exclusivo de este artículo es el establecer perentoriamente que deberán *bloquearse* cuando no se pueda establecer su exactitud o su vigencia sea dudosa, y en cualquiera de ambos casos no corresponda su *cancelación*²⁹.

Lo que también es nuevo y exclusivo de este artículo es el establecer que el responsable del registro o banco de datos deberá eliminar, modificar o bloquear de oficio los datos personales —“sin necesidad de requerimiento del titular” dice la ley—, y la sanción al efecto está señalada en el artículo 23º, esto es, que se deberán indemnizar los daños patrimoniales y morales que se causen por el tratamiento indebido de los datos.

11. CONSAGRACIÓN DE LA OBLIGACIÓN DE SECRETO

El artículo 7º establece que las personas que trabajen en el tratamiento de datos personales, tanto en organismos públicos como privados, estarán obligadas a guardar *secreto* sobre los mismos cuando provengan o hayan sido recolectados de fuentes no

²⁷ El inciso tercero del artículo 12 señala que “sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos”.

²⁸ El inciso segundo del artículo 12 repetirá más adelante que “en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen”.

²⁹ El artículo 15º establece que “no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional”, y que “tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva”.

accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con la base de datos, obligación que no cesa por haber terminado sus actividades en ese campo³⁰.

Creemos que se trata de una mera declaración de principios o de la consagración de una confidencialidad de alcances muy restringidos, toda vez que la regla general en la ley aprobada es que los bancos de datos sean fuentes de acceso público, y a su respecto no rige la obligación de secreto en comento.

12. TRATAMIENTO DE DATOS PERSONALES EN VIRTUD DE UN MANDATO

El artículo 8° de la ley aprobada establece que cuando el tratamiento de datos personales se efectúe por mandato se aplicarán las reglas generales; que el mandato deberá ser otorgado por escrito, dejándose especial constancia de las condiciones de la utilización de los datos, y que el mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

13. PRETENDIDA OBLIGACIÓN DE COHERENCIA ENTRE EL TRATAMIENTO DE DATOS PERSONALES Y LA FINALIDAD DE RECOPIACIÓN

Recordemos que el artículo 4° estableció, como regla general teórica, que la autorización del titular para que sus datos personales o nominativos sean tratados requiere que la persona sea *"debidamente informada respecto del propósito del almacenamiento de sus datos personales"*.

El artículo 9° por su parte, señala 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. Es decir, en estos casos se autoriza desviar o no considerar la finalidad que se tuvo —y que nunca se declaró— al momento de recopilarse. A manera de resguardo, agrega el artículo que la información debe ser exacta, actualizada y debe responder con veracidad a la situación real del titular de los datos.

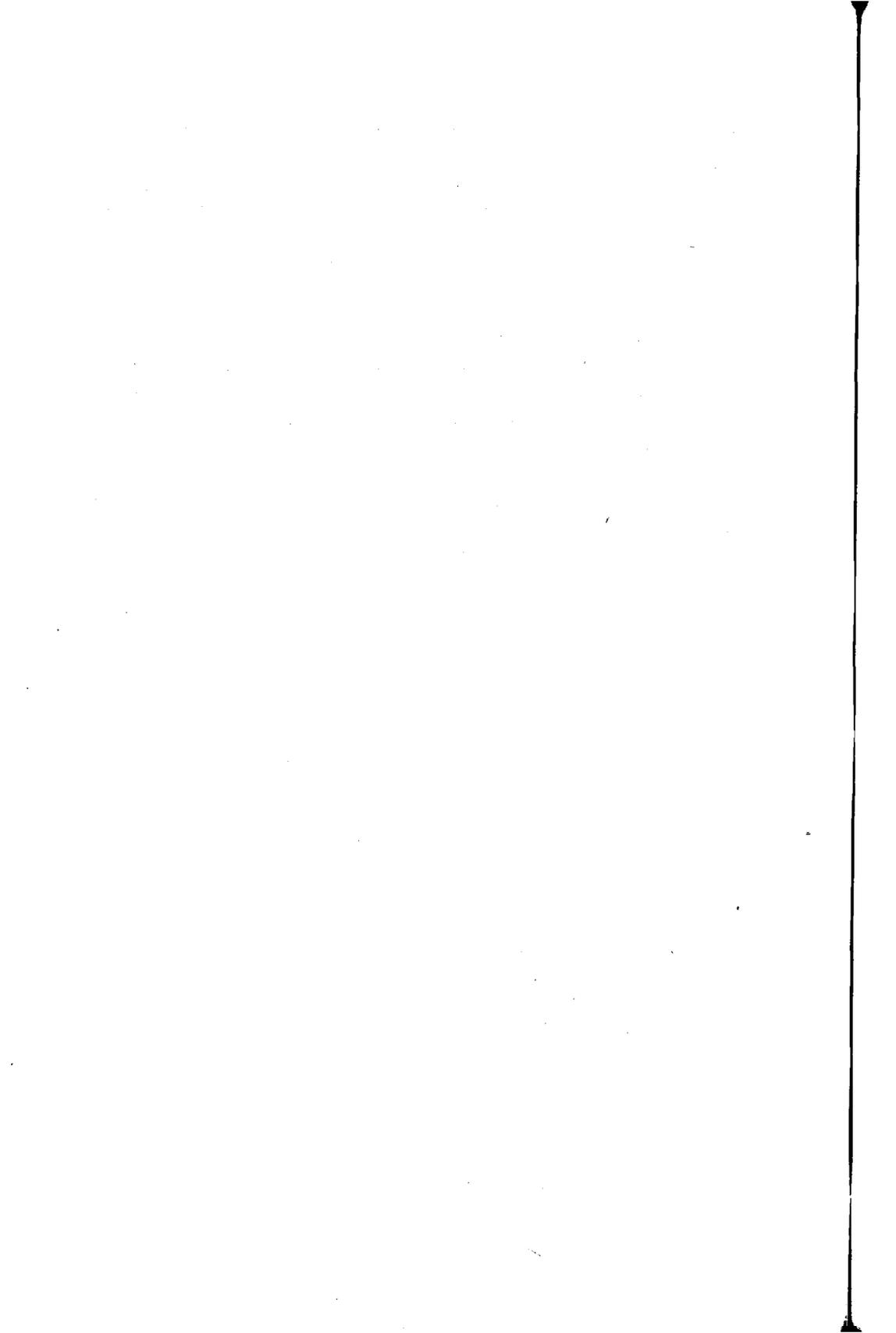
³⁰ A diferencia del artículo 10 de la Lortad de España, de donde se recogió casi íntegramente el artículo, la obligación no rige por el solo hecho de que se procesen datos personales sino que sólo respecto de lo que la nueva ley considera de acceso restringido o reservado, lo que, como sabemos, son los registros o bancos de datos de excepción.

14. REGULACIÓN DE LOS DATOS SENSIBLES "O PERSONALÍSIMOS"

Recordemos que el artículo 2° letra g) señala que son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, "tales como" los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

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

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



**DATOS PERSONALES: PROPIEDAD PRIVADA,
LIBRE INICIATIVA PARTICULAR Y RESPETO
A LA VIDA PRIVADA**

RAÚL BERTELSEN REPETTO
Profesor Derecho Constitucional
Universidad de los Andes

I. EL TRATAMIENTO DE DATOS COMO UNA ACTIVIDAD ECONÓMICA LÍCITA

**1. SIGNIFICADO Y ALCANCE DEL DERECHO A DESARROLLAR
CUALQUIERA ACTIVIDAD ECONÓMICA LÍCITA RECONOCIDO EN
EL ARTÍCULO 19 N° 21 DE LA CONSTITUCIÓN POLÍTICA**

El N° 21 del artículo 19 de la Constitución Política de la República, en su inciso primero, asegura a todas las personas “el derecho a desarrollar cualquiera actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, respetando las normas legales que la regulen”. Los titulares del derecho son, en principio, únicamente las personas privadas, sean éstas naturales o jurídicas, pero no el Estado y sus organismos, pues éstos únicamente pueden desarrollar o participar en actividades empresariales si una ley de *quórum* calificado los autoriza. Así lo dispone el inciso segundo del mismo precepto.

Como todo derecho de libertad, el de desarrollar cualquiera actividad económica lícita es un derecho que se tiene frente a todos, *erga omnes*, e implica que existe una obligación general de no hacer que recae sobre autoridades y particulares. Todos los obligados, entonces, han de abstenerse de cualquier comportamiento lesivo al derecho que se reconoce, el cual faculta a sus titulares para actuar libre de interferencias, dentro, naturalmente, de

las regulaciones legales establecidas. Pero incluso estas regulaciones, conforme lo garantiza el N° 26 del artículo 19 de la Constitución Política, no pueden ser excesivas y llegar a afectar la esencia del derecho o su libre ejercicio.

Evans de la Cuadra explica certeramente quiénes son los titulares del derecho y los obligados a respetarlo:

“Si la Constitución asegura a todas las personas el derecho de desarrollar libremente cualquier actividad económica, personalmente o en sociedad, organizadas en empresas, en cooperativas o en cualquier otra forma de asociación lícita, con el único requisito de respetar las normas que regulan la respectiva actividad [...], la obligación de no atentar en contra de esta garantía no sólo se extiende al legislador, al Estado y a toda autoridad, sino también a otros particulares que actúen en el ámbito de la economía nacional. Una persona, natural o jurídica, que desarrolla una actividad económica dentro de la ley, sólo puede salir de ella voluntariamente o por ineficiencia empresarial que la lleve al cierre o a la quiebra”¹.

Este derecho, denominado por la Comisión de Estudio de la Nueva Constitución Política de la República como “libre iniciativa privada para desarrollar cualquiera actividad económica” y usualmente “derecho a desarrollar cualquiera actividad económica lícita”, significa, entonces, que toda persona privada, sea ésta persona natural o jurídica, tiene la facultad de iniciar y mantener con libertad, exenta de toda interferencia indebida, cualquiera actividad lucrativa en las diversas esferas de la vida económica. Garantiza, por consiguiente, la norma constitucional, entre otras actividades, la explotación de recursos naturales, realización de actividades productivas, de servicios y de comercialización de todo tipo de bienes, bajo dos grandes condiciones: la primera, que la actividad a realizar no sea considerada en sí misma, ilícita, y son tales sólo las que la propia Constitución menciona genéricamente, esto es, las contrarias a la moral, al orden público y a la seguridad nacional, y la segunda, que la actividad económica a realizar se ajuste a las normas legales que la regulen.

La doctrina y la jurisprudencia han precisado el alcance con que se encuentra consagrado constitucionalmente el derecho a desarrollar cualquiera actividad económica lícita.

¹ Evans de la Cuadra, Enrique: “Los derechos constitucionales”, Santiago de Chile 1986, tomo II, pág. 318.

Es por lo tanto el del artículo 19 N° 21 de la Carta Fundamental un reconocimiento amplio, y así lo recordaron en 1996 los Tribunales Ordinarios de Justicia al acoger un recurso de amparo económico:

“...la antes referida garantía constitucional, a la que se le ha llamado de libre iniciativa o de libertad de empresa, es de contenido vasto, ya que comprende la libre iniciativa y la prosecución indefinida de cualquiera actividad económica, sea productiva, comercial, de intercambio o de servicio, habiendo sido introducida por el Constituyente de 1980 con especial énfasis y estudio, según consta de la historia fidedigna del precepto”².

El Tribunal Constitucional ha tenido igualmente ocasión de pronunciarse sobre el significado del derecho a desarrollar cualquiera actividad económica lícita. En sentencia de 21 de abril de 1992 expresó, en cuanto a la fundamentación del derecho:

“Que, el derecho consagrado en el artículo 19, N° 21, [...] y que protege la libre iniciativa privada es una expresión de los contenidos filosófico jurídicos del Capítulo I de la Constitución Política, y viene a ser una consecuencia del principio de subsidiariedad, como también del deber del Estado de resguardar el derecho de las personas a participar con igualdad de oportunidades en la vida nacional”³.

En el mismo sentido, en sentencia de 30 de octubre de 1995, al fallar el requerimiento presentado por más de la cuarta parte de los diputados contra el proyecto de ley sobre “Libertad de Expresión, Información y Ejercicio del Periodismo”, el Tribunal Constitucional expresó que el derecho a desarrollar cualquiera actividad económica lícita, “amparado y protegido por la Constitución, no es sino expresión del reconocimiento de la primacía de la persona humana y de su libre iniciativa para emprender y así realizar la plenitud de sus virtualidades para su propio bien y el de sus semejantes, colaborando en la promoción del bien común. Se trata, pues, de un derecho de fundamental importancia para los individuos al permitir desarrollar tanto el espíritu de iniciativa como la subjetividad creadora de cada una de las personas”⁴.

² Corte de Apelaciones de Santiago, sentencia de 25 de mayo de 1996, acoge recurso de amparo económico, considerando 3°. Confirmada por la Sala Constitucional de la Corte Suprema el 19 de junio de 1996.

³ Tribunal Constitucional, sentencia de 21 de abril de 1992, considerando 8°.

⁴ Tribunal Constitucional, sentencia de 30 de octubre de 1995, considerando 41°.

Los límites del derecho a desarrollar actividades económicas son, como se ha indicado, dos: que la actividad sea lícita, y que no infrinja las normas legales que la regulen. En cuanto a lo primero, Evans de la Cuadra estima que corresponderá a los tribunales de justicia pronunciarse cuándo ciertas actividades hayan de ser consideradas contrarias a la moral, al orden público o la seguridad nacional, pues existe una imposibilidad de hacerlo previamente mediante una ley.

“No creemos –dice– que sea posible una ley que complemente estas limitaciones, ya que, o bien aborda con criterio general la explicitación de los conceptos de moral, orden público, etcétera, lo que no parece propio de la tarea legislativa, o bien busca precisar las actividades específicas que serán prohibidas, lo que implica entrar en una regulación casuista imposible de concebir”⁵.

2. RESERVA LEGAL PARA LA REGULACIÓN DE TODA ACTIVIDAD ECONÓMICA. EXCLUSIÓN DE LA POTESTAD REGLAMENTARIA AUTÓNOMA Y LÍMITE DE LA POTESTAD REGLAMENTARIA DE EJECUCIÓN

Mayor interés, sin embargo, tienen las consideraciones que efectúa Evans de la Cuadra en torno a la competencia que el artículo 19 N° 21 de la Carta Fundamental confiere al legislador para regular las diferentes actividades económicas, regulación que será el marco dentro del cual aquéllas podrán efectuarse:

“Para estudiar la significación jurídica y la trascendencia práctica de este precepto, digamos, primero, que las personas que ejerzan una actividad económica deben someterse a las leyes que la *regulan*. Pues bien, “regular” una actividad es someterla al imperio de una regimentación que indique *cómo puede* realizarse; pero en caso alguno, bajo pretexto de “regular” un accionar privado en la economía, el legislador puede llegar hasta obstaculizar o impedir, a través de facultades excesivas a organismos fiscalizadores, por ejemplo, la ejecución de actos lícitos amparados por esta garantía constitucional”⁶.

Por su parte, el Tribunal Constitucional, en la sentencia de 21 de abril de 1992, se ha ocupado también de fijar el alcance de la competencia otorgada al legislador para regular las actividades económicas:

⁵ Evans de la Cuadra, op. cit., pág. 318.

⁶ Id., pág. 317. Las cursivas son del original.

“Que, del tenor del artículo 19, Nº 21, resulta que los que desarrollen una actividad económica deben someterse a las normas legales que la regulen. Por regular debemos entender, según el Diccionario de la Real Academia: “Ajustado y conforme a reglas”. De lo anterior se infiere que sujetar una actividad a una regulación significa establecer la forma o normas conforme a las cuales debe realizarse, pero en caso alguno puede ser que bajo el pretexto de regular se llegue a impedir el ejercicio de una actividad”⁷.

Posteriormente, en sentencia de 6 de abril de 1993, pronunciada, al igual que la anterior, sobre el caso de los letreros camineros, el Tribunal tuvo que volver a ocuparse del tema de la regulación de una actividad económica, lo que le dio oportunidad para reiterar y ampliar la doctrina expuesta un año antes. Así, luego de recordar la definición de “regular” que da la Real Academia en su Diccionario, reiteró que “ello no podría jamás interpretarse en el sentido de que se impida el libre ejercicio del derecho. Por otra parte, si bien al regular se pueden establecer limitaciones y restricciones al ejercicio de un derecho, éstas claramente, de acuerdo al texto de la Constitución, deben ordenarse por ley y no mediante normas de carácter administrativo”. Y poco más adelante volvió a insistir en la idea de que la regulación de una actividad no puede traducirse en un impedimento u obstáculo para la realización de la actividad regulada:

“Regular una actividad es someterla al imperio de una reglamentación que indique cómo puede realizarse, pero en caso alguno, bajo pretexto de “regular” un accionar privado, se puede llegar hasta obstaculizar o impedir la ejecución de actos lícitos amparados por el derecho consagrado en el artículo 19, Nº 21, de la Constitución Política”⁸.

Por otra parte, en sentencia de 25 de mayo de 1996 dictada por la Corte de Apelaciones de Santiago al acoger un recurso de amparo económico interpuesto por la Asociación de Exportadores y Embotelladores de Vinos A.G., sentencia que fuera confirmada por la Sala Constitucional de la Corte Suprema el 19 de junio de 1996, los tribunales ordinarios han citado y hecho suya la doctrina desarrollada por el Tribunal Constitucional sobre los límites existentes para regular una actividad económica en sus sentencias de 21 de

⁷ Tribunal Constitucional, sentencia de 21 de abril de 1992, considerando 9º.

⁸ Tribunal Constitucional, sentencia de 6 de abril de 1993, considerandos 12º y 14º.

abril de 1992 y 6 de abril de 1993. De esta forma, nos encontramos ante criterios jurisprudenciales uniformes de una y otra jurisdicción constitucional —la que está en manos del Tribunal Constitucional y la que ejercen las Cortes de Apelaciones y la Corte Suprema—, lo que no siempre ha ocurrido y que confiere, entonces, a la doctrina sustentada por uno y otras en materia de libertad económica el carácter de indiscutida.

3. LA LEY Nº 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA COMO MARCO LEGAL REGULADORIO DE LA ACTIVIDAD ECONÓMICA DE TRATAMIENTO DE DATOS

Aunque no sea su objeto principal, puesto que la ley se denomina a sí misma de protección de 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. Así aparece sobre todo en el inciso segundo de su artículo 1º al decir que “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”. Esto último es sólo reiteración del principio de supremacía constitucional consagrado en el artículo 6º de la Carta de 1980. Concordante con la disposición citada se encuentra la letra o) del artículo 2º que define lo que es “tratamiento de datos”.

En todo caso, 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 referido artículo. Lo anterior, teniendo presente que, conforme se comentará más adelante, la intervención en un ámbito privado como el de los documentos que den cuenta de dichas obligaciones sólo puede ser ordenado por ley para casos determinados con precisión.

II. EL DERECHO DE PROPIEDAD EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

1. LA PROTECCIÓN CONSTITUCIONAL SOBRE TODA CLASE DE BIENES CORPORALES O INCORPORALES

Entre los derechos reconocidos constitucionalmente que toda ley que regula una actividad económica debe respetar se encuentra el derecho de propiedad. Ello significa que la normativa legal que enmarca la realización de una actividad determinada, como es la de tratamiento de datos, no debe afectar los derechos de propiedad existentes. De ahí la necesidad de precisar cuál es el ámbito de la protección constitucional de la propiedad.

Un primer aspecto del que puede llamarse estatuto constitucional de la propiedad es el acceso amplio a la titularidad de todo tipo de propiedades. Por ello, la Constitución asegura a toda persona en el N° 23 del artículo 19 "La libertad para adquirir el dominio de toda clase de bienes, excepto aquellos que la naturaleza ha hecho comunes a todos los hombres o que deban pertenecer a la Nación toda y la ley lo declare así". Es el llamado derecho a la propiedad, que es la norma general en materia de acceso al dominio, y es la base o supuesto que permite la existencia de derechos de propiedad sobre cualquier bien susceptible de apropiación.

En el memorándum de 16 de agosto de 1978 que la Comisión de Estudio de la Nueva Constitución Política elevó al Presidente de la República con "Proposiciones e Ideas Precisas" se justifica el reconocimiento de este nuevo derecho en los siguientes términos:

"Hemos estimado conveniente consagrar en el anteproyecto como nueva garantía constitucional el derecho a la propiedad, vale decir, el de ser titular de toda forma de propiedad, sea que recaiga sobre recursos naturales, bienes de consumo, medios de producción, etc. De este modo, se consagra la capacidad de toda persona para adquirir el dominio sobre toda clase de bienes, sin perjuicio de las limitaciones que la ley establezca por exigirlo el interés nacional. Se ha querido así destacar que el régimen de propiedad privada en nuestro derecho es el básico y general"⁹.

Respecto al derecho de propiedad, la norma que lo reconoce y protege, como es sabido, es el N° 24 del artículo 19, disposición

⁹ Memorándum con "Proposiciones e Ideas Precisas", N° 56.

esta que en su inciso primero asegura a toda persona "El derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales o incorporales", que, luego, en el inciso segundo establece la regulación y, también, la limitación por ley de la propiedad para hacer efectiva su función social, y que en el inciso tercero reafirma la protección amplia de toda propiedad al disponer que "Nadie puede, en caso alguno, ser privado de su propiedad, del bien sobre que recae o de alguno de los atributos o facultades esenciales del dominio, sino en virtud de ley general o especial que autorice la expropiación por causa de utilidad pública o de interés nacional, calificada por el legislador".

La misma Comisión de Estudio al dirigirse al Presidente de la República en 1978 afirmaba:

"El precepto que os proponemos garantiza al derecho de propiedad en sus diversas especies, sobre toda clase de bienes, corporales e incorporales. En este sentido, ampara en forma amplia este derecho, cualquiera que sea su significación patrimonial o la forma de propiedad, sea esta última individual, familiar, comunitaria, etc."¹⁰.

Es comprensible que como resultado de la aplicación de las nuevas normas constitucionales relativas a la libertad para adquirir el dominio de toda clase de bienes, y al derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales e incorporales, la jurisprudencia haya reconocido y otorgado protección de modo amplísimo sobre diversos y numerosos derechos de significación patrimonial.

En tal sentido, y sin que la enumeración sea exhaustiva, puede recordarse cómo además de la propiedad de derechos reales —entre ellas la del derecho real de hipoteca y la de servidumbres— se ha admitido la propiedad de numerosísimos derechos personales, sea que se tengan respecto de un particular o de una institución pública, sin importar tampoco que tengan su fuente en contratos particulares, en la aplicación de normas legales o en disposiciones de índole administrativa. Incluso, en casos que pueden resultar audaces pero que no son sino el producto de la aplicación de las normas constitucionales a nuevas situaciones de la vida económica y social, se ha aceptado la propiedad sobre una concesión, la propiedad sobre los derechos de uso de un bien nacional de uso

¹⁰ Memorándum con "Proposiciones e Ideas Precisas", N° 68.

público, la propiedad sobre la zona de concesión otorgada a un concesionario eléctrico, la propiedad de los derechos que emanan de la calidad de estudiante, la que existe sobre el derecho a ejecutar una obra en virtud de la autorización administrativa otorgada y la propiedad sobre el derecho inmaterial de un recorrido de una línea de movilización colectiva.

Los ejemplos anteriores, que podrían alargarse fácilmente, no son sino una demostración de la amplitud con que la Constitución Política reconoce y protege el derecho de propiedad, sin que sea necesario para reconocer la existencia de una propiedad garantizada constitucionalmente que tenga un estatuto legal propio, pues basta para ello que de la vida jurídica haya surgido una situación o una relación en que concurren las características propias del dominio.

2. DERECHOS DE PROPIEDAD EN LOS REGISTROS O BANCOS DE DATOS

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. 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, esto es el uso, goce y disposición, quien podrá celebrar a su respecto los actos y contratos que permita la legislación vigente y no podrá ser privado de su propiedad sino a través del correspondiente proceso expropiatorio.

Sobre el particular es interesante recordar una sentencia de 19 de diciembre de 1994 de la Corte de Apelaciones de Santiago, confirmada por la Corte Suprema el 5 de enero del año siguiente, en que se acogió el recurso de protección interpuesto por un académico que había sido despedido de la universidad de la que era profesor. En uno de los considerandos de esa sentencia se expresa:

“Que si bien es cierto que el artículo 8° de la ley N° 17.336 (la Ley de Propiedad Intelectual) atribuye a los empleadores la propiedad intelectual de los programas computacionales generados por sus dependientes, debe tenerse presente que

tales "programas computacionales", son medios, herramientas o sistemas que permiten y facilitan a un individuo la creación de trabajos, ya sea bajo la forma de escritos, fórmulas, gráficos o en otra cualquiera que la tecnología admita, de manera tal que no cabe confundir el medio que permite la generación de tales creaciones intelectuales, con las creaciones mismas"¹¹.

Aunque el caso resuelto no es exactamente el mismo que podría plantearse en torno a la utilización de una base de datos, pues de lo que se trataba en el recurso de protección que he citado era de la propiedad de trabajos académicos, lo que plantea más bien un problema de propiedad intelectual, de igual modo, a mi juicio, correspondería dar protección jurisdiccional a la propiedad que su titular tuviera de bancos de datos personales lícitamente obtenidos.

III. EL RESPETO A LA VIDA PRIVADA EN EL TRATAMIENTO DE DATOS

1. PROTECCIÓN CONSTITUCIONAL DE LA VIDA PRIVADA Y DE LOS DOCUMENTOS PRIVADOS

El artículo 19 N° 4 de la Carta Fundamental asegura a toda persona el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

A su respecto, se presenta la necesidad de abordar el difícil concepto de privacidad y su distinción de lo público.

"Por vida privada —ha dicho la jurisprudencia— se entiende aquella zona que el titular del derecho no quiere que sea conocida por terceros sin su consentimiento, mientras que por vida pública se comprende aquella que llevan los hombres públicos y de la que conocen los terceros, aun sin su consentimiento, siempre que sean de real trascendencia"¹².

Sin embargo, puede criticarse tal definición, en cuanto la misma no es comprensiva de aquello que es natural o legalmente accesible al público, ni de lo que puede conocerse lícitamente aun contra la voluntad del interesado. En ambos casos se estaría en la esfera de lo público, con plena independencia del consentimiento o no por parte del sujeto de la información.

¹¹ Gaceta Jurídica N° 175, enero de 1995, pág. 42, considerando 3°.

¹² C. Ap. Stgo. 31-5-1993. Cit. por Cea Egaña, "El sistema constitucional de Chile", pág. 94.

Por otro lado, el artículo 19 N° 5 de la Constitución Política asegura a toda persona la inviolabilidad del hogar y de toda forma de comunicación privada. De ahí deriva la propia Carta Fundamental la consecuencia de que el hogar sólo puede allanarse y —en lo que interesa para el objeto de este trabajo— que las comunicaciones y documentos privados únicamente pueden interceptarse, abrirse o registrarse en los casos y formas determinados por las leyes.

El término “documentos” fue utilizado en un sentido amplio por los redactores de la Constitución, y es así que en la sesión N° 129 de la Comisión de Estudios de la Nueva Constitución se dijo que comprendía no sólo los diplomas, cartas, relaciones o escritos que ilustren acerca de algún hecho, sino cualquier cosa que sirva para comprobar algo, incluso las grabaciones¹³. Está fuera de toda duda, por consiguiente, que dentro de los documentos privados a que se refiere la Constitución Política están incluidos los que son propios de los negocios de una sociedad comercial como son la cartera de sus clientes.

En cuanto al alcance de la garantía constitucional sobre inviolabilidad de los documentos privados existe coincidencia en que por regla general su acceso está vedado y que sólo excepcionalmente, y siempre que lo decida una ley dictada conforme a la Constitución, podrá accederse a los mismos.

Evans de la Cuadra, que integraba la Comisión de Estudios en la época en que ella se ocupó de la garantía que protege a los documentos privados, precisa en los siguientes términos su alcance:

“Como regla general, puede establecerse que los recintos privados, las comunicaciones y los documentos personales, familiares y de trabajo no pueden ser allanados, interceptados, abiertos, registrados o conocidos, *salvo que algún texto legal lo autorice, para casos determinados y de excepción y con formalidades que eviten o impidan el abuso o la arbitrariedad*”¹⁴.

La jurisprudencia ha aceptado igualmente que los documentos mercantiles están amparados por la garantía constitucional que resguarda la privacidad. Es por ello que el acceso a los mismos sólo es posible cuando una ley limitativa del derecho que se asegura —la inviolabilidad de los documentos y comunicaciones privados—, dictada respetando las garantías que para este tipo de legislación contem-

¹³ Acta oficial correspondiente a la sesión N° 129, pág. 23.

¹⁴ Evans de la Cuadra, op. cit., tomo I, pág. 177. El énfasis es nuestro.

pla el N° 26 del artículo 19 de la Carta Fundamental, esto es que no los afecte en su esencia ni en su libre ejercicio, lo autorice, pues si ello no ocurre no es lícito el conocimiento de los documentos privados.

En tal sentido cabe recordar la sentencia de 4 de enero de 1995 del Tribunal Constitucional, que estimó contraria al N° 5 del artículo 19 de la Constitución Política la disposición contenida en la nueva ley de drogas que facultaba a la autoridad administrativa el conocimiento amplio de documentos mercantiles de las personas investigadas por el Consejo de Defensa del Estado.

El precepto cuestionado, a juicio del Tribunal, resultaba inconstitucional porque “no contempla en forma íntegra, completa y exacta el procedimiento ni los casos precisos cómo debe aplicarse”. En dicha situación, “al no especificarse el procedimiento y no señalarse los casos precisos en que las medidas proceden, se está vulnerando la inviolabilidad de las comunicaciones y documentos privados, que sólo pueden interceptarse, abrirse o registrarse en los casos y formas determinadas por la ley”¹⁵.

Como es indiscutible que el término “documentos privados” incluye los registros y la documentación de una casa comercial relativos a la cartera de sus clientes cualquiera sea la forma como se guarden los mismos: en libros, papeles o archivos computacionales, por tal razón, el conocimiento de los documentos de una sociedad comercial únicamente procede ateniéndose a las exigencias que la Constitución establece y que la doctrina y la jurisprudencia han precisado. Ello implica que ha de ser la ley —nunca la autoridad administrativa—, y sólo para casos determinados en ella misma en todos sus aspectos y de acuerdo a las formalidades que precise, la que establezca cuándo procede el conocimiento de los documentos y los procedimientos a aplicar para acceder a los mismos. Si esto no ocurre, la ley será inconstitucional porque “no contempla en forma íntegra, completa y exacta el procedimiento ni los casos precisos cómo debe aplicarse”, conforme lo expresara el Tribunal Constitucional en su sentencia de 4 de enero de 1995 antes referida.

De ahí que si la ley otorgara a un órgano administrativo facultades amplias y discrecionales para dictar las normas que regularán el conocimiento de los documentos de una sociedad comercial, con

¹⁵ Tribunal Constitucional, sentencia de 4 de enero de 1995, considerando 10°, letra c).

ese otorgamiento de atribuciones la ley infringiría la garantía constitucional de inviolabilidad de los documentos privados porque no evita o impide el abuso o la arbitrariedad. Tal sucede porque no sólo es inconstitucional la ley que derechamente permite el conocimiento indebido de documentos privados, sino, también, la que pone en peligro el goce efectivo de las libertades y derechos que la Constitución Política reconoce y asegura, según lo ha precisado el Tribunal Constitucional.

No hay que olvidar, además, que las informaciones de las casas comerciales a las que se podría acceder afectan igualmente los derechos de los clientes de aquéllas. Los clientes —recordémoslo— también gozan de la garantía de inviolabilidad de los documentos privados del N° 5 del artículo 19 de la Carta Fundamental, razón por la que es imperativo proteger a aquellos deudores de una sociedad que no han pedido información de sus deudas, pero que quedarán expuestos al peligro de que terceros conozcan su situación de endeudamiento.

Los créditos otorgados y las deudas existentes entre una sociedad que otorga financiamiento a sus clientes con recursos propios o de otra sociedad con la que está relacionada, forman parte de una relación privada, voluntariamente contraída. Es, pues, una relación de confianza cuya reserva debe cautelarse de modo especial del conocimiento de terceros.

2. RESPETO A LA VIDA PRIVADA Y RESGUARDO DE LA PRIVACIDAD DE LOS DOCUMENTOS EN LA LEY N° 19.628

Para abordar esta materia es preciso analizar en particular las disposiciones del Título Primero de la ley. Un aspecto central en la estructura de dichas normas es el concepto de “datos personales” o “datos de carácter personal”. Según la letra f) del artículo 2° de la ley, datos personales son “los relativos a cualquier información concerniente a personas naturales, identificadas o identificables”. Con ello, parece excluirse la protección de los datos que conciernen a personas jurídicas. Surge entonces la duda acerca de si el derecho de toda persona al tratamiento de datos del artículo 1° de la ley no contendrá una restricción inconstitucional al no permitir que se traten datos de personas jurídicas.

Los datos personales, definidos en el párrafo anterior, pueden en general ser clasificados en tres grupos, según su índole y procedencia, a saber:

a) Datos personales que provengan o se recolecten de fuentes accesibles al público

Según la definición de la letra i) del artículo 2º, fuentes accesibles al público son “los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes”. Tales datos, en los supuestos del artículo 4º, inciso quinto, de la ley, no requieren autorización de su titular para ser objeto de tratamiento.

Dichos supuestos, conforme a la norma legal mencionada, ocurren cuando los datos son de carácter económico, financiero, bancario o comercial; cuando se contienen en listados relativos a una categoría de personas que se limitan a indicar antecedentes tales como la pertenencia del individuo a un grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, y también cuando son necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta de servicios.

De lo expuesto resulta, entonces, que los datos mencionados en el inciso quinto del artículo 4º de la ley, cuando se obtienen de fuentes accesibles al público, no requieren de la autorización de su titular para ser objeto de tratamiento.

b) Datos personales en general

Los datos personales en general, esto es, todos aquéllos no comprendidos en el inciso quinto del artículo 4º –referido a datos obtenidos de fuentes accesibles al público–, por una parte, y tampoco los que queden incluidos dentro de la categoría de datos sensibles de la letra g) del artículo 2º; por otra, pueden ser utilizados por las personas responsables de un registro o banco de datos en los casos y bajo las condiciones que contempla la Ley Nº 19.628.

El artículo 4º, inciso primero, de la ley, prescribe en tal sentido 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”. En otras palabras, existe un tratamiento de datos que es lícito realizar sin la voluntad del titular de los mismos, y otro que únicamente es lícito efectuar previa autorización de los titulares de los datos.

Casos en que la ley permite efectuar tratamiento de datos sin que sea necesario contar con la autorización de sus titulares son los contemplados en el inciso sexto del artículo 4º y en los artículos 17 a 19 de la ley.

La primera de las disposiciones citadas excluye de la necesidad de 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 beneficios de carácter general de aquéllos".

El segundo grupo de disposiciones se refiere, por su parte, a las informaciones que versen sobre obligaciones de carácter económico, financiero, bancario o comercial contenidas en los documentos protestados a que se refiere el artículo 17, o las informaciones que den cuenta del incumplimiento de las obligaciones de dinero a que se refiere esa misma disposición.

A su vez y conforme a lo dispuesto en el artículo 4º de la ley, el tratamiento de datos personales con autorización de su titular exige que ella reúna las siguientes características:

- i) consentimiento expreso del titular de los datos;
- ii) consentimiento manifestado por escrito;
- iii) consentimiento informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público;
- iv) autorización vigente o no revocada por escrito. Además, otras disposiciones contenidas en el título I de la ley "De la utilización de datos personales" imponen diversas obligaciones a las personas u organismos responsables de registros o bancos de datos, entre las que conviene destacar las contenidas en el artículo 7º, que impone el deber de guardar secreto sobre los datos personales recolectados de fuentes no accesibles al público a las personas que trabajan en el tratamiento de los mismos, y en el artículo 9º que establece la obligación de utilizar los datos personales sólo para aquellos fines para los que fueron recolectados cuando no provienen de fuentes accesibles al público.

c) Datos personales sensibles

Los datos sensibles, por último, definidos en la letra g) del artículo 2º, en principio no pueden ser objeto de tratamiento según lo dispuesto en el artículo 10 de la ley, aunque esta disposición contempla luego algunas excepciones que en cierta manera aproximan los datos sensibles a los datos personales privados en general.

Datos sensibles, según la norma legal que los define, son “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual”. Como puede apreciarse de la definición citada, estos datos constituyen un conjunto restringido dentro de la totalidad de los datos personales, ya que, aunque participan de lo que distingue a estos últimos que es la referencia a cualquier información concerniente a una persona natural, identificada o identificable, son relativos a determinadas informaciones más íntimas o privadas de las mismas.

No es extraño, por consiguiente, que la Ley N° 19.628 haya tenido el propósito de ser más restrictiva en el tratamiento de datos personales. Al respecto, el artículo 10 de la misma dispone que “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”.

A modo de conclusión, de las normas examinadas precedentemente es posible colegir tres principios claves en la ley:

1° Tratándose de datos personales que provengan o se recolecten de fuentes accesibles al público (artículo 4° inciso quinto), la ley establece amplios supuestos en los cuales el tratamiento no requiere autorización de su titular.

En efecto, en estos casos no se requiere autorización del titular cuando se esté en presencia de alguno de los tres tipos de datos a que se refiere el inciso quinto del artículo 4° de la Ley N° 19.628, y que son: i) los de carácter económico, financiero, bancario o comercial; ii) los que se contengan en listados relativos a una categoría de personas y 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, y iii) los necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, esto es los datos para el *marketing* directo.

En los demás casos, los datos recolectados de fuentes accesibles al público requerirán autorización para su tratamiento, tal como se

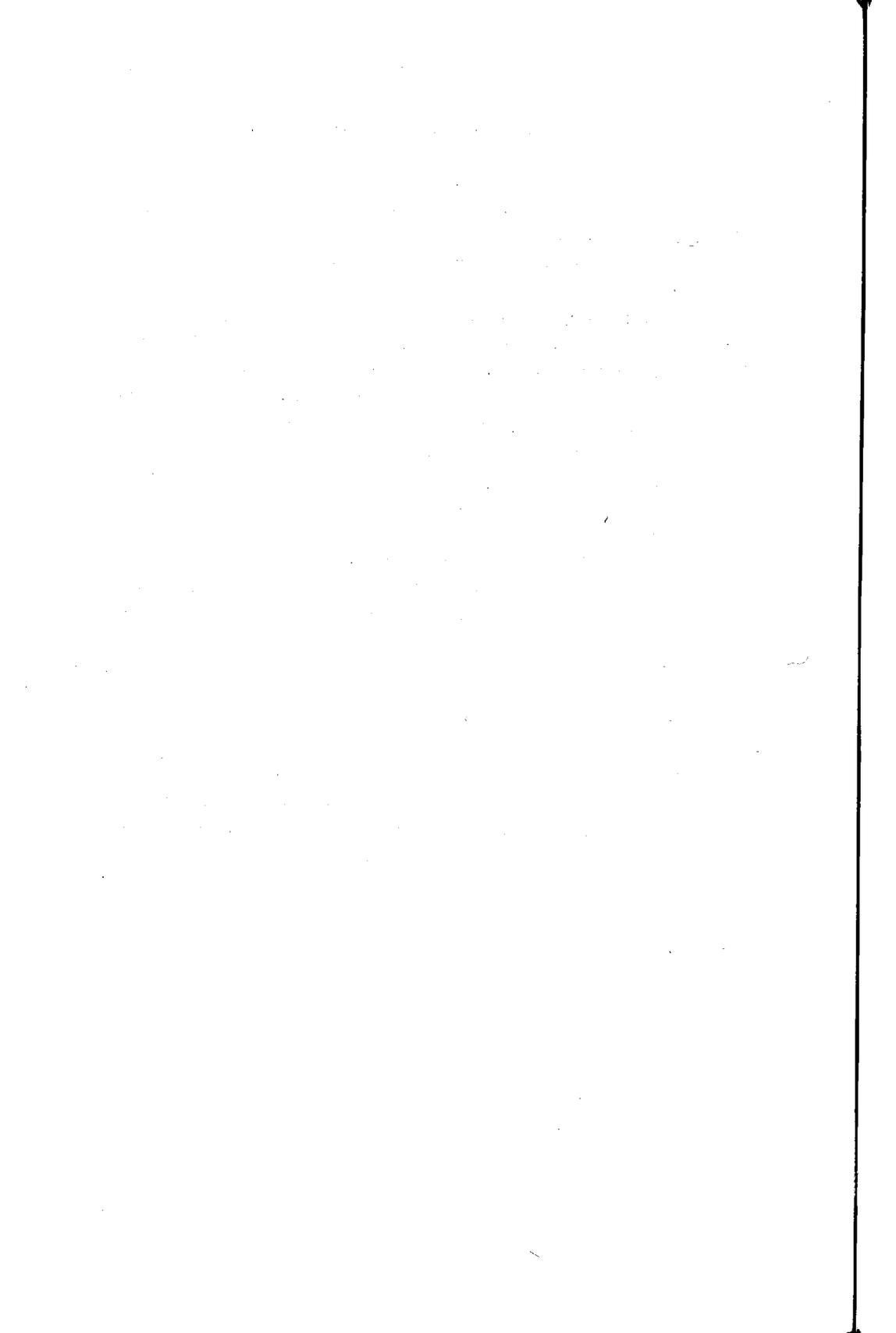
dispone para los datos, llamémosle privados, según se comenta a continuación.

2° En el caso de los datos personales que no provienen o son recolectados de fuentes accesibles al público —datos privados—, el tratamiento puede efectuarse sólo con consentimiento de su titular, por regla general.

Excepcionalmente, el artículo 4° inciso primero, explicado más arriba, excluye de la necesidad de contar con la autorización de su titular el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que estén afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

También por vía de excepción y según ya se ha comentado, el tratamiento de estos datos puede efectuarse sin mediar autorización del titular cuando la ley en comento u otras lo autoricen; como ocurre en los casos de comunicación de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, reguladas en el título III de la ley.

3° Finalmente, tratándose de los datos sensibles, definidos más arriba, éstos en principio no pueden ser objeto de tratamiento (artículo 10°), pero luego la misma disposición contempla diversas excepciones que los aproximan a los datos personales privados. Por consiguiente, la autorización del titular para su tratamiento debiera sujetarse a los términos del artículo 4, comentados con anterioridad. Lo anterior, sin perjuicio de los casos en que conforme al propio artículo 10 u otras disposiciones legales estos datos sensibles puedan ser objeto de tratamiento.



RÉGIMEN DE LOS BANCOS DE DATOS DE ORGANISMOS PÚBLICOS. UNA APROXIMACIÓN DEL DERECHO ADMINISTRATIVO A LA LEY SOBRE PROTECCIÓN DE LA VIDA PRIVADA

RAMIRO ALFONSO MENDOZA ZÚÑIGA*

Profesor de Derecho Administrativo

P. Universidad Católica de Chile

Universidad de los Andes

I. INTRODUCCIÓN

Datos, información e informática son conceptos cuya relación ha avanzado abruptamente en la nueva modernidad; sin embargo, no nos hemos percatado realmente de ello. La individualidad de la persona humana, entendida ella misma como un elemento digno de clasificación o dotada de atributos o bienes clasificables y cuantificables (datos), siempre ha sido una zona de interés tanto privado como público; sin embargo, por factores de tiempo, espacio, o legitimidad, no siempre ha sido posible aunarlos de manera que esa información se pueda conocer, recopilar y almacenar en forma ordenada, acabada, segura y lícita.

La verdadera incidencia de la manipulación de datos por parte de entidades públicas o privadas, al parecer, no fue correctamente dimensionada sino hasta el advenimiento de la llamada "era de la información", donde la tecnología permitió que pudiera almacenarse toda clase de datos y, más aún, hizo posible que éstos se mantuvieran siempre conectados con la persona respecto de la cual provienen, sin importar el registro o base de datos en la cual se encuentren y el titular de la misma.

* El autor agradece, especialmente, la colaboración de su ayudante de investigación, Sra. Blanca Oddo Beas (P. Universidad Católica de Chile).

Ante esta tecnología y posibilidades que ella brinda, la informática ante el derecho¹ presenta una variedad de enfoques, todos de gran trascendencia. Desde luego, un elemento que trae a colación es su directa relación con el poder, puesto que quien es dueño de la información es precisamente quien la controlará, usará según sus propias finalidades y, por ello, se encontrará en inmejorables condiciones de imponer su voluntad; y otro elemento que resulta por lo demás ser correlativo al ejercicio del poder descrito es aquel referido a los derechos de los individuos y los roces que surgen en la relación existente entre la protección de sus derechos, la privacidad de los datos que a aquél se refieren (se trata de la creación de un sistema de protección de datos) y el derecho de los demás, de ser informados respecto de los datos registrados acerca de las personas.

Como vemos, en este tema poder y derechos fundamentales se encuentran en íntima imbricación, lo que al menos permite aventurar, a modo conclusivo, que cuando son los órganos del Estado los que detentan la información es el Derecho Público el instrumento adecuado para lograr de esta estrecha unión una articulación legítima en miras de propender al bien común y, por ende, al servicio a la persona humana. Este es el fin que justifica la acción del Estado, y que además, siendo su deber alcanzarlo, no le es posible excusar su ejercicio en cuanto existan los presupuestos para su actuación, lo que en este caso se da a todas luces.

De esta forma se advierte cómo ha sido posible que en el derecho de la Administración se encuentren temas cada vez más modernos o tecnológicos. En efecto, al menos en las fronteras del tema que ahora trataremos, normativamente se han implementado varias novedades, desde el uso de la firma digital y los documentos electrónicos por los órganos del Estado², la instalación de un portal de compras del Estado, hasta la definitiva protección legal de los datos de carácter personal, por la nueva Ley N° 19.628, sin omitir, desde luego, las importantes imposiciones de *transparencia docu-*

¹ Sobre esta materia vid. José Manuel Castells Arteché, *La limitación Informática*, en Estudios sobre la Constitución Española, Homenaje al profesor Eduardo García de Enterría, t. II, "De los Derechos y Deberes Fundamentales", Civitas (1991), pp. 907-941; también Fernando Sáinz Moreno, *Secreto e Información en el Derecho Público*, op. cit., tomo III (1991), pp. 2863-2981.

² Al efecto, vid. D.S. N° 81 (Segpres), de 10 de junio de 1999, pub. en Diario Oficial de 26 de junio de 1999, que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado. De interés también D.S. N° 5.996 (Interior), de 24 de septiembre de 1999, pub. en Diario Oficial de 12 de noviembre de 1999.

*mental*³ que, ahora como principio, se encarga de contemplar la Ley de Bases, luego de las modificaciones que le introdujera la llamada Ley de Probidad Administrativa⁴.

Se trata, entonces, de un tema nuevo que requiere de ciertas advertencias, especialmente en lo que respecta al problema de la influencia extranjera, específicamente, en cuanto a cuál es el elemento histórico al que se debe recurrir en su interpretación, ya que si se analiza el texto de la ley, al parecer se da el terreno propicio de una verdadera importación indiscriminada de dogmáticas foráneas, en particular, de la legislación española⁵. También se denota lo impropio de esta regulación a nuestro ordenamiento jurídico, en la circunstancia de que, en verdad, en todos los países en que se prevé una normación de esta especie, a diferencia del nuestro, existe una ley general de procedimiento administrativo y, además, hay un régimen legal único y ordenado del tema, mas no la verdadera dispersión de normas que en nuestro país aparecen contenidas en esta ley, las que también, como señalábamos, forman también parte de la Ley 19.653, sobre probidad administrativa.

En esta ley confluyen muchos aspectos relacionados con la protección de la persona, y es esta perspectiva desde la cual deben ser interpretadas sus normas; así también deben serlo aquellas otras contenidas en cuerpos legales o normativos distintos que afecten esta protección; es lo que sucede, por ejemplo, con el actual artículo 13 (antiguo 11 bis de la Ley 18.575), de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, precepto que faculta a los órganos del Estado para declarar ciertos actos bajo la condición o calidad de *secretos*, cuestión que pugna claramente con el derecho que asiste a los particulares en razón de la Ley 19.628 (sobre protección de datos personales), para conocer

³ Habíamos anunciado esta necesidad de transparencia en mi *Notas sobre el acceso a la documentación administrativa (acerca de la publicidad, la transparencia y el secreto)*, en Revista de Derecho Público (U. De Chile), vol. 1996, N° 59, p. 243 y ss.

⁴ Se trata de la Ley 19.653, de 14 de diciembre de 2000. Su Reglamento sobre el Secreto o Reserva de los Actos y documentos de la Administración del Estado, en D.S. N° 26 (Segpres), de 28 de enero de 2001, pub. en Diario Oficial de 7 de mayo del mismo año.

⁵ En España, numerosa bibliografía sobre la materia ha sido desarrollada últimamente. De utilidad, *El derecho a la intimidad y a la privacidad y las Administraciones Públicas*, obra colectiva, director Domingo Bello Janeiro, Manuel Heredero, coordinador, Santiago de Compostela, 1999. En especial, *Los derechos de la persona en el ámbito de las tecnologías de la información*, de Eduardo Vilariño Pintos, pp. 17-30; *La relación jurídica de disposición de datos de carácter personal*, Francisco González Navarro, pp. 31-80, entre otros.

y requerir de la Administración los datos contenidos en registros públicos ya sean propios o de terceros en cuanto por su naturaleza y finalidad interesen para el desarrollo de ciertas actividades.

Sólo a esto nos dedicaremos en los acápitos que a continuación siguen⁶.

II. ¿MATERIA DE LEY?

Sabido es que el legislador no puede ejercer su potestad en todas las materias. La actual Constitución innovó en la materia y restringió la dictación de leyes estableciendo el llamado dominio legal máximo, dicen algunos; es decir, se fija un límite al legislador, y se especifica en su texto cuándo es posible dictar leyes. En tal sentido, su artículo 60 dispone que *sólo son materias de ley* las siguientes. Con este imperativo se pretendió prohibir al legislador inmiscuirse en ámbitos respecto de los cuales no estaba expresamente autorizado por la misma Constitución.

Ante este enunciado, lo primero que cabe preguntarse es si las materias que contiene la Ley 19.628, sobre protección de datos personales, son, propiamente, materias de ley o, lo que es lo mismo, de dónde arranca la competencia del legislador para la presente regulación.

Desde luego, es evidente que esta competencia no se desprende explícitamente del mencionado artículo 60 de la Constitución, cuestión que pudiera llevar a la conclusión apresurada de que la materia no es propia de la ley; suerte que este postulado, bajo esta sola reflexión, no podría ser real, ello debido a que el pretendido propósito del dominio máximo que estatuye en su enunciado el artículo 60 de la Constitución, ya citado, tampoco lo es. El mismo artículo en su numeral 20 abrió la potestad legislativa de modo general a *toda*

⁶ Nuestro esfuerzo no está destinado a determinar el contenido del derecho a la privacidad y la honra, curiosamente, tan vinculados con los esfuerzos de transparencia y publicidad que toda esta nueva legislación promueve. Sobre el contenido del derecho señalado, de utilidad Revista Jurídica Ius et Praxis (U. De Talca), año 6, N° 1, 2000, su número monográfico *Libertad de opinión e información y derecho a la privacidad y a la honra*, dedica gran parte de sus páginas (502) a este cometido. Desde una perspectiva del derecho civil, aunque con incursiones en el marco de lo público, Hernán Corral Talciani, su *Vida familiar y derecho a la privacidad*, en Revista Chilena de Derecho (PUC), 26 N° 1 (1999), pp.76 ss; también su *Configuración jurídica del derecho a la privacidad II, concepto y delimitación*, en Rev. Chilena de Derecho (PUC), 27 N° 2, (2000), 331-355, ambos con abundante derecho comparado.

otra norma general y obligatoria que estatuya las bases esenciales de un ordenamiento jurídico y, además, porque la Constitución en muchas materias encarga directamente al legislador que las regule, en forma exclusiva y excluyente, como es el caso del ejercicio de los derechos fundamentales que se reconocen en el artículo 19, entre otros.

Debemos detenernos entonces en otras *materias de ley* que están y se cruzan preferentemente en toda la Constitución. Muchas de ellas, como lo hemos señalado, establecidas en el artículo 19. Dice allí que la Constitución asegura a todas las personas los derechos que en esa extensa norma se reconocen. Aquí hay dos tipos de normas, algunas que hacen referencia al legislador, vale decir, facultándolo para que éste precise la forma en que se debe desarrollar la actividad que constituye el derecho de que se trata y, las otras, que contienen referencias directas a su regulación intrínseca, es decir, se refieren al contenido mismo del derecho.

Por ejemplo, las disposiciones del artículo 19 N° 11 inciso 4º, N° 12, N° 21, N° 24 señalan que tales actividades se realizan *en conformidad a la ley*. Asimismo, el N° 15 del mismo artículo prescribe sobre el derecho de asociación que las entidades que allí se reconocen deben "*constituirse en conformidad a la ley*". En cambio, el N° 24 inciso 2º señala que sólo la ley puede introducir el *modo de adquirir*, de manera tal que dicha definición conceptual de adquisición del derecho está entregada en plenitud al legislador.

Desde luego y por lo dicho, podemos afirmar que la Ley 19.628 no encuentra su fundamento o soporte en considerarla como una ley que regula una *actividad económica* en los términos que considera el artículo 19 N° 21 de la Carta, aunque así lo entiendan algunos esta conclusión es errónea. En efecto, este indicado precepto constitucional reconoce y asegura el derecho a desarrollar cualquiera actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, *respetando las normas legales que la regulen*. Esta regulación, debemos admitirlo, no se refiere al ejercicio externo del derecho, lo que exigiría que la ley normara su ejercicio, sino que al contenido interno de la actividad en sí: v.gr. la actividad económica de distribución eléctrica, que aparece intensamente regulada por el legislador; la actividad económica que surge en el ámbito del servicio sanitario también resulta esencialmente regulada, desde el tipo societario que corresponde asumir al prestador hasta el minucioso detalle tarifario que el legislador traza para esta actividad. En aquellas legislaciones se definen normalmente y

con detalle los contenidos internos del derecho y las restricciones y condiciones de ejercicio del mismo; en otras palabras, se definen los contenidos de la actividad económica que el legislador ha conceptualizado. De tal manera que las definiciones externas a este contenido no son propiamente preceptos legales que regulen una actividad económica⁷.

Que esta ley no esté basada en el artículo 19 N° 21 de la Constitución es de importancia fundamental, y su consecuencia más relevante podemos, a estas alturas, adelantarla: de aquí se deriva la premisa de que no hay una autorización del Estado para desarrollar una actividad que considere materias reguladas por esta ley y, además, que tampoco se requiere esta intervención para la concreción de aquellos actos que digan relación con la transferencia o la cesión económica de los datos que por la misma ley se protegen.

Una correcta apreciación de la fuente constitucional de la que emana su regulación legal parte por analizar el objeto de esta ley. Pues bien, ésta trata de la vida privada de las personas, garantía que está consagrada en el artículo 19 N° 4 de la Constitución, conclusión que se vislumbra prístina de su propia denominación: *protección de la vida privada* y, bien sabemos, que la vida privada ha sido tratada en dicho artículo. Pero, nuevamente, debemos poner en evidencia que en este numeral no hay referencia o convocatoria a la ley, de donde se sigue que la fuente de esta legislación, para su creador, está –lisa y llanamente– en una aplicación directa de la Constitución, puesto que el legislador no ha sido convocado mediante el clásico reenvío –técnica usual del constituyente del 80– puesto que particularmente respecto a este derecho la norma constitucional se satisface a sí misma, sin convites de ninguna especie.

En este punto conviene tener a la vista el artículo 19 N° 26 de la Constitución, el cual señala que los preceptos legales pueden regular garantías, pero también pueden “*complementar garantías*” y esta es, precisamente, una ley que complementa la garantía indicada.

Luego se está complementando un derecho. Complemento es añadir algo, ampliarlo, mejorarlo, por lo que a través de ella se trata de resguardar la vida privada de las personas a tal punto que

⁷ Sobre esta diferencia de aplicación del artículo 19 N° 21 y el contenido de la regulación, de suma utilidad Iván Aróstica Maldonado, su *Derecho Administrativo Económico (Libre iniciativa privada y actividad empresarial del Estado)*, Universidad Santo Tomás, Escuela de Derecho, 1ª. Ed. (2001), en especial 71-86.

ni siquiera sus disposiciones se aplican a las personas jurídicas, sólo a las personas privadas, naturales. Todo su contenido ha sido para ampliar y mejorar el derecho garantido y de acá que, en estricto rigor, esta ley no es una ley que verse acerca de la pluralidad informativa, ni respecto de la transparencia de actos del Estado, sino que se refiere, exclusivamente, acerca de la persona, su personalidad y su privacidad.

Pero curiosamente la protección de la vida privada se rescata con un criterio de nimiedad. Se protege o amplía frente a datos personales y nos obnubilamos con referencias tales como lo "económico", lo "financiero", "lo bancario" y "lo comercial". Sin embargo, se olvida que esa información normalmente la tienen los particulares, y aún más que en *strictu sensu* ella es intrascendente para la libertad y vida de las personas, salvo por el acceso al crédito o la molestia de recibir cartas no deseadas en nuestro domicilio.

Estos elementos son francamente irrelevantes en la vida de las personas, pues el verdadero peligro está en el poder y la información personal que acerca de nosotros posee el Estado. Es normalmente el burócrata quien llega a nuestras profundas intimidades y ahí, curiosamente, se produce una suerte de ruptura respecto del criterio de bilateralidad que, al menos formalmente, se quiso enunciar en su tramitación de modo tal que, en rigor, esta ley omite desarrollar esta esfera de custodia que explicaría y fundamentaría, con creces, su dictación.

III. LA ACTIVIDAD REGISTRAL DE LA ADMINISTRACIÓN Y LA PUBLICIDAD DE REGISTROS

La Ley 19.628, sobre Protección de Datos de Carácter Personal, nos habla de registros o bases de datos, en ocasiones indistintamente, lo que nos lleva necesariamente a tener que indagar en torno a la actividad registral de la Administración.

Es un hecho cierto que el Estado es quien tiene la mayor cantidad de registros⁸ de datos, son la propia naturaleza y finalidad

⁸ Sólo por vía ilustrativa podemos señalar los siguientes: Registro Nacional de Servicios de Transporte de Pasajeros, Registro Internacional de Obras Audiovisuales y su Reglamento, Registro de Consultores del Ministerio de Planificación y Cooperación, Registro Nacional de Contratistas de Gendarmería de Chile, Registro de Consultores del Ministerio de Obras Públicas, Registro de Corredores, Registro Nacional de Contratistas de

de sus órganos los elementos que determinan que sean estos entes los que con mayor facilidad puedan recoger antecedentes relativos a las personas y por ende mantenerlos en archivos y registros⁹, las más de las veces, además, unido al condicionante fundamental que significa el hecho de que para ejercer determinadas actividades deba en forma previa sindicarse y anotarse a la persona en Registros que lleva e impone la misma autoridad.

La ley habla, impropriamente, de registros o bases de datos como una expresión de sinonimia, aunque es evidente que ambos conceptos son distintos. Mientras la voz "registros" denota un conjunto organizado de datos de carácter personal, los "bancos de datos" imponen un concepto más especializado que comprende a un fondo común de datos, característica que comparte con los registros, pero que se diferencia de ellos porque son accesibles a varios usuarios. Es en este último sentido en el que parecen haber sido tomados los registros que se tratan en este cuerpo legal. Así por lo demás lo demuestra la práctica legal chilena.

Por su parte, los datos a los que se refieren estos registros o bases de datos han sido también incorrectamente conceptualizados. De esta manera la ley los agrupa bajo la nomenclatura "de datos de carácter personal" o sencillamente "datos personales"; enseguida, los define sin distinción como aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables", siendo que en doctrina son tratados separadamente, ya que, por un lado, no siempre los datos personales son datos de carácter personal, y así viceversa.

Trabajos Topográficos y Jurídicos, Registro de Productos Agropecuarios; Registro Nacional de Acuicultura, Registro Nacional de Condenas por Violencia Intrafamiliar, Registro Nacional de Condenas, Registro General de Contratistas de Carabineros de Chile, Registro Especial de Faltas por Tráfico ilícito de Estupefacientes y Sustancias Psicotrópicas, Registro Nacional de Constructoras de Viviendas Sociales, Registro Nacional de Órganos Técnicos de Capacitación, Registro Nacional de Embarcaciones Artesanales, Registro Nacional de Subsidios Habitacionales, Registro de Afiliados a Juntas de Vecinos, Registro de Certificación de Exportación, Registro Nacional de Receptores de Órganos, Registros de Producción Pecuaria, Registro Municipal de Carros y Remolques, Registro Nacional de Armas, Registro de los Contribuyentes, Registro Nacional de Telecomunicaciones, Registro de Naves y Artefactos Navales, Registro Nacional de Criadores y Engoraderos Porcinos, etcétera.

⁹ La doctrina al respecto distingue ambos conceptos, ya que los Registros Públicos se diferencian de los archivos públicos en que los registros confieren efectos jurídicos a los actos-pactos, o simples datos que a ellos se incorporan, mientras que los archivos son simples conjuntos orgánicos de documentos reunidos para su conservación y ulterior utilización. Sobre este punto vid. Fernando Sáinz Moreno, *Secreto e Información en el Derecho Público*, cit.

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

- Datos personales *stricto sensu*, que son los datos existenciales, en la medida en que (y sólo cuando) pueden ser asociados a una persona identificada o identificable; v.gr., nacimiento, muerte, estado civil, domicilio, etc.;
- Informaciones sobre cosas y bienes, lo que se revela en la ley con bastante amplitud y que constituye "cualquier información", y
- Ejercicio de determinadas actividades.

Sin embargo, esta enunciación no es comprensiva de todos los datos que es posible referir a una persona; así también pueden ser objeto de un registro o bases de datos, por ejemplo, la información numérica, alfabética, digital (huellas) o acústica, y en general toda aquella información que pueda ser recogida y almacenada.

Asimismo, mención aparte merecen los llamados datos sensibles, los que sí son propiamente datos personales, y en tal sentido son definidos por la ley como "*aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o síquicos y la vida sexual*".

Desde otro punto de vista, el llamado dato de carácter personal puede ser de dos clases: dato accesible al público y dato no accesible al público; esta diferenciación nos revela un aspecto de la actividad registral, entendiendo por ella no el registro de las personas, sino que la incorporación de un grupo de personas, bienes o actividades a un instrumento que se va a llamar registro y que traduce una significativa circunstancia: dicha actividad no es, necesariamente, un camino de publicidad de información, sino que más bien puede ser de limitación o de regulación del derecho, mas no de transparencia de la gestión administrativa.

Lo anterior indica que la existencia de un registro público no traduce como equivalente significado que su contenido sea necesariamente público, sino que la denominación es identificatoria de una situación orgánica. Se trata, entonces, del órgano público que contiene o mantiene ese registro para el cual el acceso de los particulares a la información contenida en ellos es regulada por las normas particulares que rijan para cada uno en particular, porque así lo exige el principio de competencia para el cual cada órgano

tiene funciones propias y por ello cada registro que lleven ha de tener también una configuración peculiar y cumplir esa función específica, que, por de pronto, legitima su existencia¹⁰. De allí que existan:

- Registros públicos-públicos;
- Registros públicos, con listado público que lo acompaña;
- Registros públicos, de acceso restringido, y
- Registros públicos, de acceso único o reservado.

Entendida de esta forma la denominación pública de los registros que ordena la Administración cabe desechar de plano una relación intrínseca entre su regulación (fundada en el ánimo de dar protección a la vida privada) y la publicidad y transparencia de la actuación del Estado, exigida por la Ley 18.575, de Bases Generales de la Administración del Estado.

En el seno mismo de la Comisión Constituyente se planteó la problemática descrita (información manejada por un órgano público), pero a raíz de otra discusión, que fue la de la garantía constitucional del artículo 19 N° 11, acerca de la libertad para informar y emitir opinión. En esa ocasión se criticó duramente el concepto propuesto para esa norma de "*fuentes accesibles a todos*". Se dijo que ella no podía entenderse genéricamente como *aquellos documentos o fuentes de información que son públicos* pues ese sentido era peligroso y por eso se intentó desestimar, ya por su amplitud, ya por la dudosa aplicación práctica que pudiese tener un mandato de esa naturaleza.

Sobre esas consideraciones, Alejandro Silva Bascuñán expuso ante la Comisión lo superfluo de tales justificaciones y solicitó el mantenimiento de la expresión, pues insistía en su aclaración de que aunque no existiera la obligación de informar, ella sí se plantea a los órganos públicos en relación con sus competencias, debido a que de otra manera se haría imposible el ejercicio de la libertad de opinión. En su parecer el legislador debía ser el encargado de establecer las situaciones en las que hay obligación de no informar, y a *contrario*

¹⁰ Cabe en este punto recordar que los registros públicos se caracterizan por la atribución de consecuencias jurídica al asiento, anotación, inscripción o entrada en los mismos. Tales consecuencias van desde el simple comienzo o interrupción de plazos hasta el efecto constitutivo de derechos. En este sentido los registros más importantes serán aquellos que atribuyen mayores consecuencias jurídicas a su anotación.

sensu de lo anterior, respecto de los órganos públicos, viene el grado de esfera que les corresponde en la accesibilidad. Si se quita esta frase no existiría más influencia en la materia que la dada a los Tribunales de Justicia, cuestión del todo poco recomendable.

Por eso le pareció que era necesario mantener el encargo al legislador para que éste establezca las excepciones respecto a los casos en que existe la obligación de no informar. Porque si bien están de acuerdo en que no existe la obligación genérica de informar, hay casos, tanto para los órganos públicos como para los privados, en que existe la obligación de no informar —el secreto profesional, la reserva en materia de seguridad, etc.—, que puede afectar tanto a los particulares como al Estado. Por eso que las “*fuentes accesibles a todos*” es una referencia al encargo al legislador y a la naturaleza de las cosas¹¹.

El sistema chileno actual de tratamiento de la información está fundamentalmente regulado en esta ley y en las normas dispersas que se le refieren¹². Por su parte la Ley 18.575, sobre Bases Generales de La Administración del Estado, en los artículos 11, 11 bis y 11 ter —que le incorporara la Ley 19.653¹³—, los cuales presuponen los principios de transparencia y publicidad de los actos de la Administración y sus fundamentos tratan, asimismo, de la información que maneja la Administración y el deber de darla a conocer a quienes lo requieran, a menos que concurran ciertas causales de justificación que la releven de este mandato. De esta manera reco-

¹¹ El anteproyecto elaborado por la Comisión de Estudios de la Nueva Constitución no se extendió a las fuentes de información o como en algún momento se expresó a las fuentes accesibles a todos, puesto que luego de significativas sesiones, primó un criterio orientado más a la noticia periodística que al derecho de las personas frente a la información de que dispone el Estado, en relación a los intereses de los sujetos. A mayor abundamiento, don Alejandro Silva Bascuñán en la sesión 234, de 20 de julio de 1974, señaló que “*todo órgano del Estado tiene obligación de informar veraz, oportuna y objetivamente, en cuanto a los asuntos de su respectiva competencia, sin otras limitaciones que las derivadas del orden público, la seguridad nacional y la vida privada de las personas en las situaciones que la ley contempla el resguardo a los mismos valores*”.

¹² En efecto, existen otras normas que antes sustentaban el tratamiento de la información por parte de los órganos del Estado, así la ley 18.834, Estatuto Administrativo, en su artículo 55 h) impone como obligación a cada funcionario “guardar secreto en los asuntos que revisten el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales”, por cierto que en esta parte fue bastante más generoso en la creación de medios de establecimiento de reserva que su antecesor, el DFL 338/60 que consignaba sólo a la naturaleza y a la instrucción como habilitantes de tal reserva. Por su parte el D.S. 291 de 15 de febrero de 1974 consignó que los documentos y oficios se clasificarán en secretos, reservados y ordinarios.

¹³ Vid. DFL 1/19.653, de 13 de diciembre de 2000 y pub. en Diario Oficial de 17 de noviembre pasado.

noce la posibilidad de que los órganos del Estado constituyan secretos o reservados ciertos actos cuestión que si observamos la Ley 19.268 comparten similares fundamentos en el caso de tratarse de actos que afecten a la persona en su vida privada y que por lo mismo sean secretos.

Ello se encuentra justificado por el artículo 6° de la Constitución, el que prescribe que en todo caso la Administración está sujeta directa y expresamente a la Constitución, y por ello, le corresponde a ella —y sus funcionarios— el deber de resguardar el ámbito de intimidad de aquellos terceros que le han proveído de datos e informaciones personales. De allí surge que, primeramente, existen los asuntos reservados por naturaleza, respecto de los cuales los funcionarios están en el deber de mantenerlos dentro de la esfera de intimidad que corresponde, de modo tal que si se vulnera este deber, aparte de las responsabilidades funcionarias que corresponden, el Estado está en el deber de reparar el daño que se ocasiona, por aplicación directa de los artículos 6° y 7°, en sus correspondientes incisos¹⁴.

Además esta restricción a la publicidad encuentra su fundamento en la ley, ya que es sólo esta norma la que puede encargarse de establecer el secreto o la reserva de determinadas materias, y las autoridades administrativas podrán hacerlo sólo en cuanto hayan recibido el encargo del legislador para así disponerlo¹⁵. En algunos casos la ley impondrá la plena publicidad de un registro, siendo tal publicidad uno de los fines de la creación del mismo; en otros, se exigirá acreditar un interés, pero en todo caso se protegerá la intimidad y la vida privada del titular de esa información.

En definitiva, son numerosos los registros públicos que se contienen en el ordenamiento chileno por parte de la Administración,

¹⁴ Vid. mis *Notas sobre el acceso a la documentación administrativa (acerca de la publicidad, la transparencia y el secreto)*, cit.

¹⁵ Sobre las limitaciones a la publicidad conviene tener presente los dichos del profesor Silva Bascuñán (sesión 233, de 15.7.1976) en la Comisión de Estudios de la Nueva Constitución, "...en su opinión, el legislador ya tiene una serie de casos en los cuales está perfectamente establecido el derecho de no informar: toda la esfera de lo que corresponda a la reserva y al secreto, que está en la Constitución y en las leyes. De manera, entonces, que no hay problema alguno en cuanto a que vaya a quedar en descubierto toda racionalidad por falta del encargo del legislador. Se trata, precisamente, de permitir a este que en el futuro establezca, por norma expresa y dentro de los valores que constitucionalmente se consignaran, las reglas que podrían impedir la información. A su juicio, es muy importante que sea el legislador quien asuma esta tarea. Se sabe que, para negar en concreto esta información, debe existir una determinada autoridad o persona que niegue la información y esa está basada en la ley".

fundamentalmente en una trilogía que da cuenta de: actividades, de bienes, de personas. Muchos de ellos han sido eliminados de una plumada por su manifiesta innecesaria y vocación burocrática de sus tenedores¹⁶.

IV. ACTIVIDAD REGISTRAL Y PRINCIPIO DE LEGALIDAD

A. DE LOS REGISTROS

Es un hecho conocido que la Administración registra. Cabe preguntarse ¿cómo y cuándo establece registros? La búsqueda de la respuesta a estas interrogantes hace necesario indagar acerca de la actividad registral y el principio de legalidad, o lo que es lo mismo, cuál es la fuente de la actividad registral.

Hay un problema de sentido común: si la vida privada está garantizada en los términos del artículo 19 N° 4 de la Constitución, pareciera que al menos cuando la Administración se inmiscuye en lo que hace una persona, en lo que tiene o bien, quién es, sólo lo puede hacer a partir de una especial habilitación normativa, es decir, de una atribución, o lo que es igual de una potestad y, por ello, al menos en nuestro ordenamiento jurídico, por vocación expresa del principio de juridicidad¹⁷, es siempre la ley la que debe considerar la creación del Registro.

Es innegable que esta regulación nace del ejercicio de una potestad y, siendo las potestades materia de ley al claro tenor del artículo 62 inciso 4° N° 2 de la Constitución, en relación con el artículo 7° de la misma, esta habilitación orgánica se fundamenta, innegablemente, en el principio de competencia. Este poder jurídico, además, tiene una finalidad la cual está dada por el artículo 19 N° 4 de la Constitución. En efecto, es la protección de la persona respecto de sus datos personales como corolario del derecho constitucional al respeto de la vida privada el contenido garantístico que justifica la expresa y previa habilitación de la ley en el tema que nos ocupa.

¹⁶ Vid. D.L. 2.950, que eliminó de una plumada aquellos registros que dificultaban el libre ejercicio de actividades económicas consistentes en oficios de carácter artesanal y sujetas a los llamados "carnés". Tendencia existe a la restauración de aquellas soterradas prácticas que generaban la doctrina de los favores gremiales o sindicales.

¹⁷ Vid. Eduardo Soto Kloss, su *Derecho Administrativo, Bases Fundamentales, Principio de Juridicidad*, t. II, 1ª edición; Editorial Jurídica de Chile, 1996.

Siendo así, se advierte que la Constitución, como la norma fundamental que es, obliga de manera directa y por las normas legales dictadas en su conformidad. Esta primacía se erige aun con mayor fuerza en lo que respecta a los derechos fundamentales que en ella se reconocen y amparan de manera tal que éstos nunca pueden ser afectados por la acción estatal, sea ésta proveniente del legislador, cuando por su mandato puede regular un derecho, o sea por el administrador, cuando le empece el deber de respetarlo en los términos que señale la misma Constitución y la ley.

En nuestro ordenamiento, dadas estas consideraciones, jamás podrá existir una regulación de un derecho fundamental por la vía de la potestad reglamentaria, ya que ello sólo es competencia del legislador. Por tanto, es natural que esta prohibición, de carácter constitucional, se dé en el ámbito de la protección de la vida privada y, por consiguiente, en todas aquellas materias que pudieren afectar su consagración, aun de manera indirecta.

Por su parte la existencia de un registro público se justifica por la existencia de cierta información que, referida a la persona, es manejada porque así lo implica la naturaleza del órgano del Estado que la tenga, o bien porque es de utilidad para el cumplimiento de los fines o funciones de dicho órgano, el que dentro de su competencia atesora estos datos. La especialidad de esta información está en el hecho de que ella en sí dista de ser un elemento carente de contenido por la particular esencialidad que les da su titular, y que por ello su uso o recopilación no debiera ser dejado a la discrecionalidad de un ente, del que bien sabemos está a su servicio, y no es dueño de mandar por sí mismo lo que le plazca saber de las personas.

Y es que es del caso recordar que en la protección efectiva de la persona respecto de la información que a ella se refiera se debe considerar que también existe un interés social general, o un interés particular de terceros que, en determinados casos, puede legitimar su conocimiento general o restringido, cuestión que puede fundar que en algunas ocasiones se esgrima esta finalidad para crear indiscriminadamente registros que en vez de ser instrumentos para la consecución de un fin o función, sean el pretexto de una interrupción inadecuada de la vida privada. Por ello es necesario cumplir el mandato constitucional en orden a que toda garantía constitucional debe ser complementada, regulada o afectada, principalmente por la ley, lo que exige, a su vez, que la creación de estos registros públicos sólo encuentre su fuente en esta clase de normas.

En esto hay confusión. Existe una cierta tendencia a justificar la idoneidad del Reglamento en esta materia, en cuanto éste pueda crear registros. Si bien es clara la intención del constituyente, las relaciones entre ley y reglamento no suelen ser cordiales, ya que *“parece ser algo atávico el que el Administrador no sienta ningún agrado en ser un ejecutor fiel de la ley, ni se sienta engrandecido en su función de servidor y, por el contrario, pretenda de manera constante, frecuente y reiterada ir más allá del texto que ejecuta, y simplemente legisla, vulnerando así la Constitución y la ley, y, usualmente, los derechos de la personas”*¹⁸.

Pero lo cierto es que, en todo caso, los registros públicos —mayoritariamente— aparecen creados directamente por el legislador¹⁹. De donde se sigue que dicho rango normativo es el que reconoce la idoneidad para su establecimiento, rango indiscutible que no puede desconocer la situación que se presenta en aquellos supuestos contractuales, que hacen nacer registros privados que surgen, precisamente, gracias a la relación jurídica que se origina como consecuencia o con ocasión del reconocimiento a la persona física de su derecho a disponer de sus propios datos de carácter personal. Es necesario tener muy presente que este derecho de disposición no es una facultad otorgada por la propiedad o derecho de dominio sobre esa información, sino que es un derecho que forma parte del libre desarrollo de la personalidad y como tal integrante de los conceptos de privacidad e intimidad.

¹⁸ Eduardo Soto Kloss, *Ley y Reglamento*, en Revista Ius Publicum N° 3, 1999 (Univ. Santo Tomás), pp. 33-47.

¹⁹ Como ejemplos de registros creados por ley encontramos, entre tantos otros, los siguientes, Registro de Propiedad Industrial, Registro de Propiedad Intelectual, Registro de Marcas creados por la Ley 17.288, Registro Nacional de Subsidios Habitacionales, creado por la Ley 19.281, cuyo artículo 51 impone al Ministerio de Vivienda y Urbanismo la obligación de crear y mantener este registro; Registro Público de Tierras Indígenas, en la Ley 19.253, por el artículo 15 se impone a la Corporación Nacional de Desarrollo Indígena el deber de abrir y mantener un registro en el cual se inscribirán todas la tierras a que alude el artículo 12 de la misma ley; Registro Nacional de discapacidad creado por la ley 19.284 artículos 46 y 47; Registro de Propiedad de Variedades Protegidas lo dispuso la Ley 19.342 que reguló los derechos de los obtentores de nuevas variedades vegetales; el Registro Nacional de Conductores de Vehículos por la Ley 19.495, en ella se facultó al Ministerio de Transportes y Telecomunicaciones y a Carabineros para tener un acceso directo; Registro Nacional Pesquero Industrial, Ley N° 19.079 artículo primero N° 10; Registro de Servicios de Transporte de Pasajeros de Santiago, Ley N° 19.110, artículo primero letra B; Registro de la Ley de Pesca, Ley N° 19.079, artículo primero N° 53; Registro Nacional de Martilleros, Ley N° 18.118, Título II, y, Registro de Partidos Políticos, Ley N° 19.603, artículo cuarto, entre numerosos otros.

El aspecto más importante de estos registros privados es el vínculo obligacional que se da entre el responsable del registro y el titular de los datos proporcionados; en este caso también le compete al responsable el deber de mantener reserva de los datos que le han sido confiados, y de la misma forma, manejarlos y administrarlos de conformidad a lo convenido. Estos temas necesitan también de regulación toda vez que, aun cuando exista un principio de voluntad o consentimiento en ello, es la misma garantía constitucional la que se compromete, y que por tanto debe ser protegida ante abusos de particulares²⁰.

De esta forma reconocemos solamente registros creados por ley o por la convención, de conformidad a la ley.

Por otra parte, ordenada su creación por el legislador, distinto es que el reglamento se introduzca en el marco procedimental que ha de seguirse para la correspondiente incorporación del ciudadano, del bien o la actividad en el Registro cuya orden legal de nacimiento tradujo una norma de preciso rango legal.

En esta misma línea de apego y vigencia al principio de legalidad apuntaba también un famoso autor chileno, Fernando Fueyo Laneri, en su ya clásica obra *"Teoría General de los Registros"*²¹, que es la única que en nuestro derecho mediante el estudio sistemático de los Registros trata, hasta donde alcanza mi conocimiento, precisamente, de construir los principios dogmáticos del Derecho Registral; la verdad, todo un avance del derecho en nuestra región.

Pero hay otro razonamiento que nos lleva a la legalidad. Es evidente que no pueden dos fuerzas normativas concurrir al tratamiento de una misma materia. Algo así como el que llega primero. Es por ello que se debe enmarcar un criterio: o puede la Administración vía reglamentaria establecer los registros o dicha materia es de exclusiva reserva legal.

En cuanto se ha producido una numerosa regulación legal que establece registros, es evidente que el legislador está yendo más

²⁰ Así lo corrobora la historia de la ley, la que al respecto señala: *"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 les aplican a los organismos públicos y a los particulares. No hay regulaciones separadas o diferentes, que permitan a unos inmiscuirse con 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 su familia"*. Boletín N° 896-07, Informe de Comisión Mixta.

²¹ Editorial Astrea, Buenos Aires, 1982, 248 pp.

allá de ese dominio máximo legal que hoy día se pregona. Efectivamente, lo que está ocurriendo es que se está reconociendo desde el punto de vista de las atribuciones, es decir, desde el punto de vista de las potestades, que la obligatoriedad particular del desarrollo de una actividad registral que implica la transferencia o incorporación de ciertos datos que son propios a la persona humana (derecho subjetivo) involucra necesariamente una relación entre los artículos 62 inciso 4º N° 2 y 19 N° 4 de la Constitución. Si dicha incorporación resulta obligatoria, dicha potestad sólo puede encontrar abrigo en la ley.

B. DE LAS BASES DE DATOS

Un punto distinto son las bases de datos. Hemos ya señalado que en estricto rigor la acepción registro y bases de datos son diferentes. Estas últimas son la información que recaba la Administración para el funcionamiento de ella misma, la que puede ser objeto de tratamiento, esto es, *de 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 de cualquier otra forma.*

Reconozcamos, desde ya, que al tenor del artículo 20 de la Ley 19.628, *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 que la misma ley establece. En esas condiciones no necesitará consentimiento de su titular.* Así las cosas, al tenor de la ley, las bases de datos se pueden crear por el propio desarrollo de la actividad propia del ente. No obstante, aunque la ley no lo diga, es menester hacer presente que las leyes se han referido expresamente autorizando su creación, v.gr., Ley 19.212, que crea la Oficina de Informaciones.

Ahora si la ley ha debido incorporar esta autorización legal es porque de una u otra manera sigue la idea de la expresa y previa habilitación legal, trátase como hemos dicho de potestades que se crean y que se pueden ejercer. A este respecto, la historia fidedigna del establecimiento de esta ley, en particular de este artículo 20, señala que se consideró como criterio de legitimación del tratamiento de datos la competencia del órgano que pretenda llevar estas bases y, que en relación a la habilitación legal, se optó por

desechar el principio de *especialidad*, bastando la autorización legal otorgada en términos generales.

En este sentido se dijo: "La primera parte de este artículo, que deja sujeto el tratamiento de datos personales por parte de un organismo público a aquellos que se refieran su competencia, encuentra su origen en el artículo 6 de la H. 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, N° 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". Se añadía: "Si bien es una norma que puede estimarse innecesaria, al tenor del artículo 7° de la Constitución Política, presta utilidad su inclusión en un cuerpo legal que por primera vez da reglas en forma sistemática de los datos personales, más aún si se considera que numerosos organismos públicos tiene solamente normas de carácter reglamentario sobre la materia o, incluso, ni siquiera de esa jerarquía".

Enseguida, se hizo referencia al tema de la legalidad de las bases de datos, aceptándose una pretendida competencia implícita de la Administración para ello, echando por tierra el principio de especialidad en la materia, de esta manera se dijo que: "La tercera parte del artículo 20, al expresar que, en esas condiciones, no se necesita el consentimiento del titular para tratar sus datos personales, se inclina por el predicamento del artículo 6 de la H. Cámara de Diputados, en orden a que los distintos organismos públicos pueden tener todos los registros o bancos de datos personales que sean necesarios para el cumplimiento de sus funciones. Se desecha, de esa forma, la exigencia adicional planteada en el texto del tercer trámite constitucional, en cuanto a que, además de la habilitación legal general para realizar su cometido, cada organismo público requiriese otra, específica, que le permitiese organizar y mantener bancos de datos personales. Entendió la Comisión Mixta y los señores representantes del Ejecutivo que la existencia de un registro general de bancos de datos personales del sector público, prevista en artículo 22 de la misma proposición del Ejecutivo, así como los diferentes derechos sustantivos y mecanismos procesales que consulta este cuerpo legal, son suficiente garantía para las personas frente a los actos que la Administración realice en esta materia".

Son numerosas las críticas que se le pueden hacer a la postura del legislador, especialmente en lo que se refiere al debido complemento de la garantía constitucional del artículo 19 N° 4 de la Constitución, el cual se ve palmariamente afectado en cuanto por esta normación se permite la intromisión amplia de la Administración en la vida privada de las personas. Al desechar el principio de especialidad de la ley en la creación de bases de datos y dejar su legitimidad casi en manos del principio de competencia, el cual es medido según el órgano de la Administración que realice el tratamiento de datos, se deja un marco de discrecionalidad confiando sólo en la buena fe del órgano (se dice para el cumplimiento de sus funciones).

V. OTROS PROBLEMAS DISCIPLINARES

En este acápite, analizaremos someramente dos aspectos relacionados con los registros o bases de datos y su tratamiento por los órganos del Estado; éstos son, primero, el problema de la cesión de datos de organismos públicos y, segundo, un problema práctico atingente a la facultad de los particulares para pedir datos al Estado, y la naturaleza de los mismos.

La ley 19.628, sobre Protección de Datos Personales, al definir el concepto de tratamiento de datos incluye dentro de las formas que puede revestir dicho tratamiento el de la cesión de datos, la que se define como la transferencia de los datos desde una base de datos a otra distinta. En efecto, posteriormente, la ley trata de la cesión de datos en los registros privados o convencionales, mas respecto de la Administración no hace referencia legal alguna, más que someterla en esta regulación a las normas contenidas en "*las reglas precedentes*".

Sin embargo, y considerando el extenso análisis al principio de legalidad, no es posible suponer que los órganos del Estado que realicen el tratamiento de datos puedan cederlos a su discreción; es más, resulta forzoso concluir que la referida cesión sólo se podrá efectuar cuando la ley expresamente lo habilite para ello²². En esto hay razones de legalidad y de competencia.

²² En este sentido Contraloría General de la República no ha tenido un criterio estable. Así en dictamen 2.267 de 1998 ha señalado que el Convenio celebrado entre la Dirección del Trabajo y la Sociedad Dicom S.A., según el cual la referida Dirección envía a la

Si aceptamos que esta materia es de competencia del legislador, corresponde que él mismo delimite el ámbito de su ejercicio, y además ello implica ejercer las potestades otorgadas conforme al ordenamiento jurídico, en el cual no cabe suponer poderes implícitos. A mayor abundamiento, claros en que la regulación que se establece por esta ley no es la referida a una actividad económica en los términos del artículo 19 N° 21 de la Constitución, es pertinente afirmar que acá no se está autorizando al Estado para desarrollarla, según su naturaleza o conveniencia económica. Esto implica, por una parte, que el Estado —la Administración (y cualquiera de sus integrantes)— no puede realizar aquellos actos mercantiles que supone la cesión o venta de esta información, puesto que la ley en comento ni siquiera tiene el rango que habilita tal actividad para las personas jurídicas de derecho público y, además, porque dicho actuar por parte de los órganos del Estado importaría, lisa y llanamente, el ejercicio de potestades de las que en verdad carecen, máxime cuando ellas sólo explicarían su fin en razón de la protección de la intimidad y la vida privada de las personas.

En definitiva, son cuatro los criterios a los que se debe atender para desechar la referida pretensión: legalidad, especialidad, intimidad y el del precedente legal²³.

En segundo lugar, en lo que respeta al problema de la petición de los datos que se puede hacer a la Administración, conviene hacer una distinción básica, puesto que se podrán solicitar datos referidos a uno mismo o bien que sean de terceros y respecto de los cuales se tiene algún interés.

Es el primer supuesto el que en este estudio merece nuestra atención. La Ley 19.628 trata en el Título II "De los derechos de los

sociedad la información contenida en el boletín de infractores a la legislación laboral y previsional, quien se encarga de procesarla computacionalmente a fin de elaborar y actualizar una base de datos, que contiene íntegramente el indicado boletín, se enmarca dentro de la órbita de competencia del señalado servicio. Ello porque el mencionado convenio no impone a ese organismo público ninguna obligación de exclusividad para Dicom S.A., en cuanto a la entrega de la información contenida en el boletín, en la forma convenida con la indicada empresa, ya que persigue el mejor cumplimiento de la función pública que desarrolla la Dirección del Trabajo, información que no reviste, además, el carácter de secreta o reservada. En este caso, se trata de un convenio de prestación de servicios en cuya virtud un órgano del Estado le encomienda a una entidad privada procesar computacionalmente determinada información, sin costo alguno para éste, ya que el beneficio que obtiene la contraparte consiste en utilizar esa información en el desarrollo propio de las actividades de su giro.

²³ Así lo dispone la misma Constitución en el artículo 60 N° 10 al exigir que toda enajenación de bienes del Estado se realice por ley; el artículo 55 letra h), tampoco permite la disposición de datos por parte de los funcionarios que los manejen.

titulares de datos”, en éste se reconoce el derecho a la información y al acceso a ella por parte de las personas a cuyos datos se refieren las bases o registros, otorgando varias posibilidades relacionadas con ello, v.gr., cancelación, modificación, eliminación, etc.

La historia fidedigna de este Título señala que el H. Senado durante el tercer trámite constitucional, en su sugerencia de texto para el artículo 12, diferenció con mayor precisión las distintas situaciones que pueden darse en relación a dichos datos, esto es, la eliminación, la modificación y el bloqueo de datos; suprimió la limitación al denominado “derecho de acceso”, y reglamentó el aviso de la cancelación y la modificación a los terceros a quienes se hubiese comunicado previamente los datos personales respectivos.

Propuso, al efecto, señalar que toda persona tiene derecho a exigir a quien sea responsable de un banco de datos que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

Por su parte en la H. Comisión Mixta consideró también otro punto que fue la concordancia del procedimiento de solicitud de información, rectificación, etc., que por esta ley se establece con el proyecto (en ese momento) de Ley sobre Probidad Administrativa, especialmente en lo que respecta a las causales de denegación de la información de los datos requeridos.

De esta manera es el artículo 15 de la misma ley el encargado de imponer restricciones al ejercicio de este derecho, señalando “No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las labores fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional”.

Claro está que esta negativa se debe sujetar a lo prescrito por la ley y en caso de que no sea así el afectado puede recurrir a la Justicia de conformidad al procedimiento previsto en el artículo 16 de la misma ley.

VI. CONCLUSIONES

1. Los registros o bases de datos son, indudablemente, materia de ley. Es innegable que en cuanto la información que en ellos esté contenida se refiera a la persona humana, particularmente a su vida privada, se encuentra comprometida en su regulación, entonces, la garantía constitucional del artículo 19 N° 4 de la Constitución; y considerando que por mandato del constituyente estos derechos fundamentales son siempre materia de ley (artículos 60 N° 20, 61 inc. 2°, 62 N° 2 inciso 4°), no corresponde que estos registros sean creados por otra norma que no sea la de fuente legal.

2. Pero, además, sólo pueden *tratarse* datos personales cuando la ley lo autorice. Se requiere por tanto de ese marco autorizatorio. Ahí sí que hay un criterio de *especialidad*; no basta entonces acudir al criterio de competencia general ni para el registro, ni para el *tratamiento de datos*. En ambos casos se requiere, por parte del Estado, ley especial, ya que la propia Ley 19.628 hoy lo exige en múltiples de sus disposiciones que hacen referencia directa siempre a la fuente legal.

MODELOS COMPARADOS DE PROTECCIÓN DE LA INFORMACIÓN DIGITAL Y LA LEY CHILENA DE DATOS DE CARÁCTER PERSONAL

FRANCISCO GONZÁLEZ HOCH
Profesor de Derecho Civil
Universidad de Chile

I. PRIVACIDAD, INTIMIDAD E INFORMACIÓN DIGITAL

Parece conveniente precisar, en primer lugar, tres términos centrales del análisis comparado de la regulación legal de la información personal contenida en bases de datos: privacidad, intimidad e información digital.

1. PRIVACIDAD

La palabra "privacidad" es un neologismo surgido de una traducción o adaptación literal del término *privacy*, empleado frecuentemente en el derecho angloamericano¹. Ocurre, sin embargo, que el sentido en que un abogado formado en la tradición del *common law* emplea la palabra *privacy* es muy distinto al sentido que atribuye al término "privacidad" un abogado formado en la tradición del derecho continental (incluyendo el chileno).

De más está decir que el empleo indiscriminado de términos en apariencia semejantes pero con significados distintos puede conducir a graves confusiones, tanto en el lenguaje corriente como en el lenguaje especializado del derecho. Por eso, una tarea prioritaria

¹ Tan neologismo es que el término "privacidad" aún no había sido reconocido en la última versión del Diccionario de la Real Academia Española de la Lengua, de 1992.

del análisis legal comparado es esclarecer el sentido en que un término es empleado en cada sistema jurídico.

En el sistema jurídico del *common law*, el término *privacy* es extraordinariamente amplio, siendo muy difícil determinar con exactitud su núcleo de significado. En verdad, el término se amplió, progresivamente, hasta llegar a comprender desde aspectos penales tales como la prohibición de obtener pruebas mediante actos ilícitos (inspecciones y arrestos ilegales) hasta decisiones de carácter personal vinculadas al mundo sexual o reproductivo, como el uso de anticonceptivos e incluso el aborto (más cercano a lo que en el derecho continental sería considerado como un ámbito de "autonomía"). Entre estos extremos, se incluye también indiferenciadamente la protección de la honra, de la imagen, de la inviolabilidad del hogar, de las comunicaciones, etc.

2. INTIMIDAD

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. La palabra "intimidad" se ha extendido, en gran parte, por razones de texto, ya que la Constitución española se refiere precisamente al "derecho a la intimidad" (artículo 18.4), a partir de lo cual ha sido usado por la doctrina y la jurisprudencia.

En la doctrina comparada subsiste un intenso debate, que recorre la filosofía del derecho, el derecho constitucional y el derecho civil, respecto a si habría surgido un nuevo derecho fundamental o de la personalidad, que algunos autores denominan "derecho a la autodeterminación informativa" y otros "libertad informática", o si en la protección de la intimidad informática no habría, más bien, sino la tutela de derechos de la personalidad ya formulados (intimidad, honor, vida privada).

En esencia, el concepto de "derecho de autodeterminación informativa" fue creado por la doctrina alemana de los 70s y recogido en un famoso fallo del Tribunal Constitucional Federal, de 1983, que declaró inconstitucional la Ley del Censo de 1982, que exigía a los ciudadanos contestar unas 160 preguntas muy detalladas, imponiendo severas multas a los renuentes. El Tribunal, desarrollando el derecho al libre desarrollo de la personalidad establecido en la Constitución Federal, decidió que exigir a una persona contestar ese número de preguntas era tratarla casi como un objeto, hacerle

perder su dignidad y desconocer que la autodeterminación como persona implica la facultad de controlar qué información entrega y cuál no. El derecho a la autodeterminación informativa es concebido, así, como "una proyección de la libertad de decisión del individuo necesaria para el fomento de su bienestar privado y para el funcionamiento de una comunidad democrática"². El derecho es de carácter marcadamente político, pues constituye una esfera de libertad, esencialmente, frente al Estado³. El nuevo término fue desarrollado luego por la doctrina italiana y por algunos autores españoles, tales como Pérez Luño y Lucas Murillo, pero no es pacífico ni siquiera en Alemania, por el riesgo de convertirse en patrimonialista, porque "induce a pensar que las personas ostentan un derecho de propiedad sobre sus datos"⁴.

Por otra parte, la noción de "libertad informática" ha sido defendida por Frosini, para quien ésta es un derecho perteneciente a la personalidad moral, consistente en el "derecho de disponer de los propios datos personales, esto es, de controlar la veracidad o exactitud, de impedir la difusión si se trata de datos sensibles o reservados, de verificar la utilización para el fin autorizado"⁵.

A partir de la doctrina de la libertad informática ha ganado fuerza la idea de que a la facultad de "exclusión", que se entendía tradicionalmente asociada la intimidad como la posibilidad de impedir a otros conocer aspectos reservados de la vida, se ha agregado el poder de "control" respecto a la información, que supone un carácter positivo de verificar el uso para el cual se recogieron los datos, su exactitud, etc.⁶.

¿Cuál es la importancia práctica de que la protección de la intimidad informática constituya un nuevo derecho fundamental o derecho de la personalidad? Según los partidarios de esta tesis (Pérez Luño y Lucas Murillo, por ejemplo), de no reconocerle la calidad de nuevo derecho fundamental, la protección de la intimidad informática se debilitaría y no podría cumplir eficientemente su función de garante frente a los peligros del Estado y de las grandes

² Denninger, "El derecho a la autodeterminación informativa", en *Problemas actuales de la documentación y la informática jurídica*, Tecnos, Madrid, 1978, pp. 272 y 274.

³ Antonio Orti, "Derecho a la intimidad e informática", Ed. Comares, Granada, 1994, pág. 41.

⁴ Esta fue la razón que se tuvo en cuenta durante la tramitación de la nueva ley chilena para eliminar la referencia a la "autodeterminación informativa", transcribiéndose en el debate de la Comisión literalmente las palabras de Orti, pero curiosamente sin citarlo.

⁵ Frosini, "Il nuovo diritto del cittadino", citado por Orti., op. cit., pág. 45.

⁶ Orti, op. cit., pág. 62.

empresas, al constituirse en un mero apéndice de otros derechos constitucionales.

Lo cierto es que, más allá de que se acepte o no la teoría de la autodeterminación informativa o de la libertad informática, lo importante es que de este intenso debate el concepto de intimidad ha salido rejuvenecido y fortalecido, integrado por las dos facetas antes señaladas: exclusión (entendida como libertad negativa) y control (entendida como libertad positiva).

Así lo ha declarado la jurisprudencia del Tribunal Constitucional español, el cual, por sentencia 254/93, afirma textualmente que:

"... la garantía de la intimidad adopta hoy un contenido positivo en la forma de derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así también, derecho a controlar el uso de los mismos datos insertos en un programa informático (hábeas data).

"... Esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades meramente negativas de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vinculan directamente a todos los poderes públicos..." (fundamento jurídico 7)⁷.

En mi opinión, cuando la Constitución chilena consagra la garantía constitucional de la protección de la "vida privada" de las personas⁸ (artículo 19 N° 5) se está refiriendo precisamente a la intimidad, en el sentido en que emplea actualmente este término el derecho continental, esto es, incluyendo las facultades de exclusión y control.

Vale la pena destacar que durante la tramitación de la Ley N° 19.628 que nos ocupa, la Cámara de Diputados definió la intimidad como "el entorno inmediato y los aspectos más reservados de la vida privada y de la propia persona que todo individuo tiene derecho a mantener fuera de toda intromisión"⁹.

⁷ Tomado de Orti, op. cit., pág. 62.

⁸ Nótese que la Constitución chilena no emplea el término "privacidad".

⁹ Informe de la Comisión de Constitución, Legislación y Justicia, de 20.5.96, Boletín 896-07 (S), página 153.

Por ello, retomando las observaciones iniciales, si se intenta entender el lenguaje empleado por los sistemas jurídicos angloamericanos y por los sistemas continentales, puede decirse con propiedad que existe una relación de género a especie, de tal manera que la "privacidad" es un amplio campo del derecho, que protege distintos aspectos de la vida personal de los sujetos, incluyendo, entre otros, su "intimidad".

3. INFORMACIÓN DIGITAL

El concepto de "información digital" merece también un breve comentario, que tiene que ver con las siempre cambiantes relaciones entre tecnología y derecho¹⁰.

Así, de la misma manera en que el tratamiento legal de la "privacidad" comenzó en los Estados Unidos con un artículo escrito hace 110 años ante los nuevos peligros que se anticipaban entonces con el surgimiento de la fotografía y la prensa¹¹, el desarrollo de las nuevas tecnologías de computación y de los sistemas de transmisión de datos en los últimos 40 años ha generado también temores respecto a amenazas a la intimidad de las personas que el derecho ha debido enfrentar estableciendo reglas que ordenen y cautelen debidamente los distintos intereses y bienes jurídicos en juego.

En otras palabras, el avance tecnológico de los computadores, junto a la facilidad para comunicarlos, han provocado un enorme aumento en la cantidad de información disponible respecto a cualquier persona. Esto ha permitido a algunos sostener que vivimos en la era de la "información digital", la cual plantea desafíos antes desconocidos para el derecho de la intimidad. Como ha señalado un autor, la batalla por la intimidad en el siglo veinte ha sido una lucha por adaptar los principios sobre intimidad a los constantes avances tecnológicos¹².

¹⁰ En mi opinión, el término "información digital" tiene una riqueza descriptiva inigualable, muy superior a la de la palabra "información personal en bases de datos" (en el mismo sentido, véase, "Ser Digital", de Nicholas Negroponte, MIT, 1996).

¹¹ Me refiero al artículo de S. Warren y L. Brandeis, "The Right of Privacy", *Harvard Law Review* 4 (1890), pp.189 ss.; este artículo es citado generalmente como el punto de inicio del pensamiento jurídico respecto a la intimidad.

¹² Robert Gellman, "Does Privacy Law Work?", en Philip E. Agre and Marc Rotenberg editors, *Technology and Privacy: The New Landscape* (Massachusetts Institute of Technology, 1997), p. 203.

El concepto de información digital lleva consigo, con todo, la idea de peligro y amenaza. Como se verá, el surgimiento de las primeras regulaciones legales de la información digital fueron una respuesta al temor que generaba el uso indebido –y control por esta vía– de la información computacional.

Y ocurre que la tecnología de procesamiento y transmisión de la información digital permite hoy aquello que antes era inconcebible: construir la imagen o perfil de una persona, a partir de datos aislados y fragmentarios mediante el cruce de información de distintas bases de datos. Esa es precisamente una de las razones que tuvo presente la ley española denominada “Ley Orgánica de Tratamiento Automatizado de Datos” (Lortad), de 1992, al señalar en su exposición de motivos que:

“El progresivo desarrollo de las técnicas de recolección y procesamiento de datos y de acceso a los mismos ha expuesto la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la 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 la persona –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 facetas de su personalidad que, aisladamente consideradas, pueden carecer 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”.

La misma exposición de motivos da cuenta de los peligros y amenazas concretas que se asocian a la información digital, con las siguientes palabras:

“... La privacidad puede resultar menoscabada por la utilización de tecnologías informáticas de tan reciente desarrollo.

“Ello es así porque, hasta el presente, las fronteras de la privacidad estaban definidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

“Uno y otro límite han desaparecido hoy: las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y

acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos”.

Finalmente, conviene hacer presente que se emplea la denominación “información digital” en un sentido más retórico que estrictamente jurídico, simplemente para facilitar la exposición, entendiendo por estos términos lo que la ley denomina con el largo nombre de “datos personales contenidos en bases de datos”.

II. TENSIONES O CONFLICTOS EN LA REGULACIÓN LEGAL CONTEMPORÁNEA DE LA INFORMACIÓN DIGITAL

La regulación legal de la información digital da cuenta de dos órdenes de tensiones, una propia de relaciones entre particulares y la otra de los particulares frente al poder público¹³.

1. CONFLICTO ENTRE PARTICULARES EN EL MERCADO (DERECHO PRIVADO)

El primer tipo de conflicto, entre particulares en el mercado, deriva de que la información digital se ha transformado en un bien demandado por el mercado, en una verdadera mercancía que es objeto de transacciones y que es consumido por todo tipo de actores: bancos, entidades financieras, casas comerciales, comerciantes, supermercados, etc. A ello se suma que las nuevas tecnologías de la información han permitido minimizar el tiempo de recolección y procesamiento de datos, han disminuido significativamente los costos de transacción y, en definitiva, han permitido democratizar el crédito¹⁴.

Sin embargo, junto con estos evidentes beneficios, las tecnologías de la información también han creado nuevos riesgos o amenazas para las personas, antes inexistentes, debido a que han puesto a disposición de terceros el conocimiento de sus aspectos más reservados o íntimos con sólo apretar un botón.

¹³ José María Álvarez-Cienfuegos Suárez, *La Defensa de la Intimidad de los Ciudadanos y la Tecnología Informática*, Aranzadi, 1999, pág. 14.

¹⁴ Piénsese, por ejemplo, en la facilidad y rapidez que existe actualmente para abrir una tarjeta de crédito en una tienda por departamentos o casa comercial o para obtener un crédito, comparado con el tiempo y costo que requerían esas mismas operaciones en Chile en la década del 60 ó 70.

En otras palabras, el desarrollo de las tecnologías de la información ha cambiado de manera inadvertida pero cierta nuestra forma de relacionarnos con nuestros semejantes, haciendo que en muchos casos hayamos perdido el control respecto a lo que estamos dispuestos a que se conozca por terceros sin nuestra voluntad.

De esta manera, el mundo creado por la información digital es un mundo antes desconocido para el hombre, y el Derecho se ha visto forzado a intervenir para regular las relaciones entre los distintos interesados que forman parte del mercado.

2. CONFLICTO ENTRE SOCIEDAD DEMOCRÁTICA Y CIUDADANOS (DERECHO PÚBLICO)

Por otra parte, en el manejo de la información digital se produce un segundo conflicto, esta vez entre el poder público y los particulares. En efecto, no hay sociedad democrática que pueda funcionar sin requerir información de sus ciudadanos para los más diversos fines, tales como planificación, estadística, presupuesto, sistema electoral, programas sociales, tributación, beneficios, etc.

La tensión está dada aquí por el temor —justificado o no— de que el poder público utilice la información para fines distintos para los que fue entregada e incluso de que se emplee la información como forma de impedir el libre ejercicio de los derechos.

3. EVOLUCIÓN DE LA REGULACIÓN LEGAL DE LA INFORMACIÓN DIGITAL EN EUROPA Y ESTADOS UNIDOS¹⁵

3.1 Europa

Tanto las legislaciones nacionales internas como los acuerdos multilaterales entre los países miembros de la actual Unión Europea han tenido un enorme desarrollo en las últimas tres décadas, cuyo examen es particularmente valioso porque muestra las adaptaciones de que han sido objeto las reglas, a medida que el avance de la

¹⁵ En este capítulo he seguido, prácticamente sin modificaciones, una parte del análisis expuesto en González Hoch, Francisco, "Privacidad de la Información Digital: autodeterminación vs. commodity", Revista Jurídica de la Universidad de Palermo, pp. 77-99, Buenos Aires, 1999.

tecnología planteaba nuevos retos y mientras se acumulaba experiencia en la aplicación de las primeras regulaciones.

Estas regulaciones, desde 1970¹⁶, nacieron fruto de la reacción de temor ciudadano frente a la amenaza de creación, por parte del gobierno, de una base de datos computacional centralizada capaz de almacenar toda la información existente sobre la vida de los particulares¹⁷.

Es interesante destacar que el nombre empleado uniformemente en las regulaciones europeas, desde 1970 hasta nuestros días, para describir lo que actualmente se entiende como el derecho a controlar la información respecto a uno mismo, ha sido "protección de datos"¹⁸. Las primeras leyes no mencionaban la palabra intimidad, ni la expresión "información personal", empleada frecuentemente en la doctrina. El uso de palabras técnicas (datos, bases de datos) antes que jurídicas (privacidad, intimidad) se justifica en que las primeras leyes dictadas en Europa sobre la materia sólo buscaban regular tecnologías¹⁹. Si bien esas leyes fueron luego modificadas o interpretadas a la luz de la noción de intimidad, según se verá, los antiguos términos técnicos fueron conservados.

Desarrollo generacional de la legislación europea. La legislación de los países europeos sobre intimidad de la información (o "protección de datos") puede ser explicada históricamente como un sistema de reglas desarrollado en cuatro generaciones o etapas, marcadas por preocupaciones específicas que justificaron la dictación de nuevas normas o la modificación de las ya existentes²⁰.

La primera generación de leyes (entre 1970 y 1977) fue dictada como respuesta al tratamiento electrónico de datos por parte del gobierno y de grandes empresas. Las normas se centraron básicamente en regular esta nueva tecnología de "procesamiento electrónico".

¹⁶ Ley de protección de datos del Estado alemán de Hessen. A ella le siguieron la ley sueca de datos (1973), la ley de protección de datos del estado alemán de Rheinland-Pfalz (1974) y la ley federal alemana sobre protección de datos (1977).

¹⁷ Viktor Mayer-Schönberg, "Generational Development of Data Protection in Europe", en Philip E. Agre and Marc Rotenberg editors, *Technology and Privacy: The New Landscape* (Massachusetts Institute of Technology, 1997), pp. 219-241.

¹⁸ Ya es un lugar común mencionar —siguiendo a Spiros Simitis, el primer comisionado de protección de datos del Estado alemán de Hessen— que no son los "datos" los que necesitan protección, sino la persona con la cual los datos se relacionan. Véase Mayer-Schönberg, op. cit., p. 219.

¹⁹ Mayer-Schönberg, op. cit., p. 224.

²⁰ Mayer-Schönberg, op. cit., pp. 221-235.

De esta manera, la mayoría de las normas de la primera generación no buscaban proteger la intimidad individual sino sólo regular el rol del procesamiento de datos frente a la sociedad. La protección de datos era vista, desde esa perspectiva, como una herramienta para enfrentar el peligro que la computación representaba a través del procesamiento de información sobre individuos determinados. Las reglas buscaron fijar un "correcto uso" del procesamiento de la información, estableciendo tempranamente el procedimiento de acceso a los datos, la posibilidad de corregir la información y los mecanismos de registro y licencia previos a la recolección de la misma²¹. Por último, el cumplimiento de las reglas no se dejó entregado a los propios individuos —a quienes no se dio acción directa— sino a una agencia o entidad especialmente creada al efecto²².

La segunda generación, a cuya vanguardia estuvieron las legislaciones de Francia, Austria, Dinamarca y Noruega (dictadas entre 1977 y 1978), surgió como respuesta a la multiplicación de registros computacionales, públicos y privados, nacidos tras la invención de los minicomputadores a mediados de los setenta.

Desaparecido el temor a un registro computacional central del gobierno, la atención se centró en la protección de las personas frente al peligro derivado de la posible recolección y procesamiento computacional indiscriminado de información personal, por el gobierno o por particulares. El punto central de esa segunda generación fue el derecho de intimidad de cada ciudadano, aplicando al campo computacional conceptos como el "derecho a ser dejado solo" (de origen angloamericano) y el derecho de cada uno a delimitar su propio espacio de intimidad.

Por primera vez, la protección de datos fue vinculada explícitamente al derecho de intimidad, y éste concebido como el derecho del individuo a rechazar a la sociedad en asuntos personales²³. En este mismo sentido, a la intimidad de la información se le dio rango constitucional en Austria, Portugal y España²⁴.

²¹ Mayer-Schönberg, op. cit, p. 221.

²² Nacieron así el Comisionado de Protección de Datos en Hessen (1970), el Consejo de Inspección de Datos de Suecia (1973) y el Comisionado Federal Alemán de Datos (1977), todos ellos precursores de la más contemporánea Agencia de Protección de Datos de España (1992).

²³ Mayer-Schönberg, op. cit, p. 226.

²⁴ El artículo 18.4 de la Constitución Española de 1978 establece: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", con lo que pone de manifiesto el carácter de amenaza con que el constituyente español concibe la informática y la obligación que impone al legislador de "limitarla".

Esta generación agregó sustancia a mecanismos que antes fueron concebidos como meramente procedimentales, reconociendo no sólo la facultad del individuo para acceder y corregir su información personal, sino también la de decidir, en ciertas ocasiones, cuál información suya podría usarse y con qué fines.

De esta manera, la protección de datos, concebida originalmente sólo como un intento de regular la tecnología computacional, se convirtió en una nueva forma de libertad individual²⁵. Además de agregarle contenido, se reconoció a los ciudadanos un papel central al permitirles exigir el cumplimiento forzado de las nuevas leyes. Asimismo, se extendieron las facultades de las entidades encargadas de hacer cumplir las normas convirtiéndolas, algunas veces, en *ombudsmen* que abogaban por los derechos del afectado, y, otras veces, en tribunales en las disputas sobre violación del derecho a intimidad en la información, al ejercer facultades de interpretación con carácter vinculante de la ley²⁶.

La tercera generación nació con un fallo del Tribunal Constitucional Alemán, en 1983, que al pronunciarse sobre la Ley de Censo acuñó la expresión "autodeterminación de la información", como se examinó antes²⁷.

Con esta sentencia, la libertad individual, entendida como el derecho a excluir o rechazar invasiones a la información personal, noción típica de la segunda generación, fue transformada en un derecho constitucional mucho más participativo. Este derecho constitucional consiste, como señaló el Tribunal Constitucional, en la "aptitud de la persona para decidir por sí misma, de manera general, la entrega y uso de su propia información personal".

El mismo Tribunal estableció que todas las fases del procesamiento de la información, desde su recopilación hasta la transmisión, estaban sujetas a limitaciones constitucionales y que, por tanto, los derechos de participación del individuo debían ser extendidos a todas esas etapas²⁸. La Corte agregó que cada vez que el gobierno pidiera información personal a los ciudadanos, debía ex-

²⁵ Mayer-Schönberg, op. cit., p. 227.

²⁶ Es el caso especialmente de la Comisión de Protección de Datos de Austria, que puede decidir controversias entre particulares y autoridades públicas. También ocurre así con las agencias holandesa y noruega; véase Mayer-Schönberg, op. cit., p. 228.

²⁷ Diciembre 15, 1983, 1 BvR 209/83-NJW 1984, p. 419; véase Mayer-Schönberg, op. cit., p. 229.

²⁸ Mayer-Schönberg, op. cit., p. 230.

plicar por qué necesitaba esa información y las consecuencias específicas de la negativa a suministrarla.

Las leyes de la tercera generación se basaron en los fundamentos y decisión del Tribunal Constitucional²⁹, y se caracterizaron por el énfasis puesto en el derecho individual a la participación y la autodeterminación de la información. En palabras de un autor austriaco, ante la realidad innegable de que en la sociedad contemporánea nadie puede optar en forma seria por no participar en ella completamente, lo decisivo es que “debe darse a los individuos la oportunidad de definir la forma en que toman parte en la sociedad mediante la entrega de información personal”³⁰.

Por último, la cuarta generación de leyes europeas (1990-2000) ha tratado de superar las limitaciones de la anterior, estableciendo diferentes soluciones para enfrentar un problema clave: la débil posición negociadora en que generalmente se encuentran los individuos al ejercer sus derechos de intimidad.

Este problema ha sido enfrentado tratando de restablecer cierto equilibrio mínimo de la posición en la que se encuentra el individuo frente a las poderosas administradoras de bases de datos y fijando áreas de protección legal obligatoria³¹.

El primer mecanismo —en mi opinión, de enorme trascendencia al cambiar el eje fundante de la responsabilidad civil— consistió en crear un sistema de responsabilidad estricta (objetiva), como es el caso de la reforma a la ley alemana sobre la materia³².

El segundo mecanismo —protección de datos “sensibles”— persiguió prohibir la recopilación o mantención de ciertos tipos de datos³³. Especialmente relevante es la Directiva sobre Protección de Datos de la Unión Europea de 1995, que prohíbe el tratamiento de datos personales que revelen (i) el origen racial o étnico, (ii) las opiniones políticas, (iii) las convicciones religiosas o filosóficas, (iv) la pertenencia a sindicatos, así como el tratamiento de los datos relativos

²⁹ Se trata básicamente de reformas a leyes existentes, por ejemplo: modificación a leyes de diversos estados alemanes como consecuencia de la sentencia del Tribunal Constitucional; la modificación a la ley austríaca de protección de datos (1986); la reforma a la Ley Federal Alemana sobre protección de datos (1990), y la adopción de una garantía constitucional específica en materia de intimidad de la información en Holanda.

³⁰ Mayer-Schönberg, op. cit., p. 231.

³¹ Mayer-Schönberg, op. cit., p. 232-233.

³² Ley Federal de Protección de Datos de 1990, 7.

³³ Así ocurre con nuevas leyes dictadas en Noruega, Finlandia, Dinamarca, Bélgica, Francia e Inglaterra, que imponen prohibiciones absolutas de procesar “información sensible”.

a (v) la salud o a (vi), la sexualidad, excepto en casos específicos expresamente enumerados³⁴.

La cuarta generación impulsó la dictación de normas para ciertas áreas específicas, atendiendo a sus características particulares. Esta tendencia fue recogida por la Directiva de la Unión Europea, mediante la idea de "códigos de conducta sectoriales", por lo que es previsible que ella será la fuente de nuevas leyes nacionales europeas³⁵.

La tendencia legislativa europea más reciente apunta a separar las tareas públicas de supervisión del cumplimiento de las leyes de aquellas relativas a la decisión de conflictos derivados de violaciones a la intimidad de la información.

Subsiste, en el centro del modelo legal de protección de datos, el derecho a la participación y autodeterminación del individuo en materia de información, pero ahora apoyado y reforzado con la intervención estatal directa para dar efectividad al cumplimiento de esos derechos.

3.2 Estados Unidos

La regulación de los Estados Unidos tiene fuertes diferencias con la legislación de países europeos, como se verá al analizar la protección legal de la intimidad de la información digital en ese país en tres sedes distintas: a) leyes especiales sobre privacidad, b) principios constitucionales, y c) acciones basadas en el *common law*.

a) Leyes especiales sobre privacidad

En forma semejante a lo ocurrido en Europa, fue el temor frente al poder que podía alcanzar el gobierno al centralizar computacionalmente información privada de los particulares lo que motivó la dictación, en 1974, de la primera ley sobre privacidad (*Privacy Act*³⁶).

³⁴ Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, artículo 8°.

³⁵ Un ejemplo es la ley de Finlandia, que regula el uso de bases de datos para investigación científica, estadísticas, investigación de mercado, *marketing* directo y reportes de crédito; véase Mayer-Schönberg, op.cit., p. 241, nota 65.

³⁶ 5 U.S.C. Sec.552a (1994).

Esta ley estableció reglas generales sobre recolección, mantención, uso y entrega de información personal en poder de agencias federales. Como su objetivo principal fue restringir el uso por el gobierno de tecnología computacional para invadir la intimidad³⁷, la primera gran limitación de esta ley es que no se aplica a las relaciones entre particulares, lo que presenta una importante diferencia con las legislaciones europeas, de aplicación al sector público y privado.

La ley sobre intimidad ha sido objeto de fuertes críticas por la doctrina, reprochándosele la ausencia de una autoridad que supervise su cumplimiento y la vaguedad de sus disposiciones, muchas de las cuales se han convertido en letra muerta por carecer las agencias gubernamentales de incentivos o amenazas para cumplirlas. Se le ha criticado, asimismo, la falta de restricciones efectivas a la difusión externa de información privada fuera del ámbito o propósito para el cual esa información fue recolectada³⁸.

Con respecto a las bases de datos privadas, las leyes más importantes son:

1. La ley que regula las agencias de informaciones sobre solvencia ("Fair Credit Reporting Act", de 1970 y modificada por última vez en 1998³⁹), que incluye normas sobre acceso y corrección de datos; límites a la recopilación, uso y divulgación de información; acciones judiciales y mecanismos administrativos de cumplimiento, etc.;
2. La ley que regula la tutela de la intimidad financiera ("Right to Financial Privacy", de 1970), y
3. La ley que regula las empresas de crédito ("Equal Credit Opportunity Act", de 1977).

b) Principios constitucionales

Si bien el texto de la Constitución de los Estados Unidos no menciona la palabra "privacidad", ello no ha impedido que existan amplios debates constitucionales en su nombre, los que han abarcado desde el derecho a la reproducción (aborto) hasta la prohibi-

³⁷ Gellman, op. cit., p. 195.

³⁸ Gellman, op. cit., p. 201.

³⁹ 15 U.S.C. 1681 et seq.

ción de ser objeto de arrestos o registros ilegales. Sin embargo, en materia de intimidad de la información no existen pronunciamientos claros de la Corte Suprema⁴⁰.

c) *Acciones basadas en el common law*

Estas acciones se fundan en la amenaza de que particulares usen bases de datos computacionales en forma impropia, violando la intimidad de las personas cuya información está contenida en esas bases de datos. En un influyente artículo de 1960⁴¹, William Prosser, autor también de uno de los más renombrados tratados sobre responsabilidad civil extracontractual (Torts), clasificó en cuatro grupos los ilícitos de violación de privacidad reconocidas en el *common law*:

1. Intrusión: irrupción, física o de cualquier otro modo, en la soledad de otro;
2. Revelación pública de hechos privados: publicar información privada y ofensiva de otro, que no es de interés para el público;
3. Falsedad: publicar una opinión ofensiva y falsa sobre otro, y
4. Apropiación: usar el nombre o la apariencia de otro, sin su consentimiento, para obtener una ganancia⁴².

El problema, como lo destaca un autor, es que la protección que pueden otorgar las acciones nacidas de los ilícitos por violación de privacidad del *common law* es por completo insuficiente⁴³.

A ello se suma que las características propias de la información digital —como su utilización al interior de una organización sin manifestación externa y sin que el afectado siquiera lo sepa— hacen difícil sino imposible configurar los supuestos de hecho propios de las acciones clásicas fundadas en irrupción, divulgación pública o

⁴⁰ Gellman, op. cit., p. 201.

⁴¹ William Prosser, "Privacy", *California Law Review* 48 (1960): 383-423.

⁴² Los cuatro grupos descritos por Prosser fueron recogidos en el Restatement (Second) of Torts, sec. 652A-E (1977); para una explicación en español véase José Martínez de Pisón, *El Derecho a la Intimidad en la Jurisprudencia Constitucional*, Civitas, 1997, pp. 32-33.

⁴³ Gellman sostiene que los 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" (op. cit., p. 210).

falsedad. Por último, debe destacarse que la doctrina sostiene que en el estado actual del derecho no puede haber responsabilidad por el uso de información contenida en un registro público⁴⁴.

3.3 Comparación Europa-Estados Unidos

Resulta sorprendente constatar que, a pesar de haber surgido como respuesta a un temor inicial común —la creación de una base de datos centralizada por el gobierno— las reglas y principios sobre protección de la información personal de los países de Europa y Estados Unidos mantienen fuertes diferencias al menos en tres áreas claves:

- 1) existencia de una agencia encargada de hacer cumplir las normas;
- 2) aplicación general de las normas a bases de datos públicas y privadas, y
- 3) protección constitucional clara a la intimidad de la información.

La explicación para las diferencias entre el modelo europeo y el americano se encuentra, en palabras del profesor italiano Vittorio Frosini, en que “en la legislación federal de los Estados Unidos se afirmó en la práctica el principio según el cual ‘todo está permitido, salvo lo que está prohibido’ por una interdicción expresa y motivada de la ley; en el otro extremo, la ley federal de la República Alemana parece basada, al contrario, en la regla según la cual cualquier actividad relativa al procesamiento de datos personales ‘está siempre prohibida, salvo cuando está permitida por una autorización expresa del poder público’”⁴⁵.

III. ALCANCE DE LA PROTECCIÓN A LA INFORMACIÓN DIGITAL EN EL DERECHO COMPARADO

En el derecho comparado ocurre frecuentemente que las reglas que rigen el tratamiento y protección de información digital no están contenidas en una sola ley, sino más bien hay un sinnúmero de

⁴⁴ Gellman, op. cit., p. 210.

⁴⁵ Vittorio Frosini, *Informática y Derecho*, Ed. Temis, Bogotá, 1988, p. 120.

regulaciones, nacionales e internacionales, de distinta jerarquía, que deben ser conciliadas y armonizadas para establecer el derecho vigente a determinada actividad.

A continuación se examina, muy someramente, el caso de las reglas jurídicas que rigen para distintos tipos de bases de datos en España.

1. BASES DE DATOS PÚBLICAS (EJÉRCITO, POLICÍA, MINISTERIOS, IMPUESTOS, ETC.)

Las bases de datos creadas por Administraciones Públicas, a diferencia de las bases de datos privadas, tienen dos exigencias adicionales: (a) deben dictar un acto administrativo previo que se publica en el Diario Oficial (mientras que las privadas sólo notifican su creación a la Agencia de Protección de Datos o APD), y (b) deben presentar sus reglas de funcionamiento previamente a la APD para su aprobación (aun cuando esto se discute).

Probablemente las otras reglas más importantes son las que prohíben la cesión o transferencia de datos entre dos entidades públicas si no tienen la misma competencia, a fin de resguardar el principio de proporcionalidad y finalidad de los datos: que éstos sólo se utilicen con el fin para el cual fueron específicamente recolectados.

Asimismo, la regulación de las bases de datos públicas establecen excepciones a los principios generales y derechos de los titulares de datos personales (información, acceso, rectificación, cancelación, etc.) cuando están presentes consideraciones de interés general.

2. INFORMACIÓN JUDICIAL

Las bases de datos con información judicial están sometidas a un régimen especial, pues no se les aplican las reglas sobre APD ni el régimen de infracciones y sanciones.

Por otra parte, no es posible utilizar las bases de datos de información jurídica y jurisprudencial para determinar la solvencia patrimonial de una persona.

3. INFORMACIÓN SANITARIA

A propósito de la información sanitaria se presenta específicamente el problema de balancear los intereses de confidencialidad del paciente y el interés general de la comunidad.

Así, las excepciones a la prohibición de tratamiento informático de datos personales relativos a la salud abarcan lo necesario para la prevención o diagnóstico médico, para prestar asistencia sanitaria o tratamiento médico y para la gestión de servicios sanitarios.

Existen también reglas especiales en materia de donaciones de órganos y gametos, reproducción de embriones, historias clínicas, biotecnología, etc.

4. INFORMACIÓN GENÉTICA

Esta es una de las áreas de mayor crecimiento y desarrollo, y debido a los avances de la investigación científica se han aprobado convenios internacionales para proteger la intimidad de la información genética, la que puede permitir construir un perfil de personalidad o físico de evidente interés laboral, sanitario, educacional, médico, etc.

5. COMUNICACIONES ELECTRÓNICAS

Las comunicaciones electrónicas, tanto vía correo electrónico como por Internet, presentan, de manera modernizada, el antiguo problema de la violación de correspondencia.

Las reglas aquí atienden a encriptar la información, establecer mecanismos de firmas digitales y, en definitiva, permitir el desarrollo de las comunicaciones y del comercio mediante comunicaciones electrónicas, protegiendo debidamente la intimidad de los que se comunican a través de la red.

6. INFORMACIÓN DE CARÁCTER COMERCIAL

La ley española (Lortad) contiene breves reglas específicas respecto a servicios computacionales sobre solvencia patrimonial y de crédito.

La información se puede obtener de fuente accesibles al público, procedentes del afectado o con su consentimiento (aun cuando esto es raro). También pueden obtenerla del acreedor, cuando se trate de obligaciones de dinero. Lo importante es que en estos casos debe notificarse a los afectados dentro de treinta días del hecho de haber sido incluidos y de su derecho a recabar información (28.1)

Si el afectado lo pide, el responsable le comunicará los datos, así como las evaluaciones y apreciaciones sobre él durante los últimos 6 meses y el nombre y dirección del cesionario.

Por último, las bases de dato comerciales (privadas) así como las bases de datos públicas están sometidas a un sistema de Registro General de Ficheros, de consulta pública y gratuita.

IV. PRINCIPIOS Y REGLAS EN LA REGULACIÓN DE LA INFORMACIÓN COMERCIAL DIGITAL EN EL DERECHO COMPARADO

1. PRINCIPIOS DE PROTECCIÓN DE INFORMACIÓN DIGITAL

En la legislación comparada se han establecido diferentes mecanismos para prevenir violaciones a la intimidad de la información personal que puedan derivarse del tratamiento computacional de datos. Si bien la extensión de la protección y los instrumentos legales específicos varían de un país a otro, pueden reconocerse en todos ellos características comunes que manifiestan la preocupación por el peligro que el uso de información digital puede significar para la intimidad.

Los mecanismos legales consisten básicamente en los resguardos para el procesamiento computacional de información, y la "acción de *habeas data*" que permite a una persona conocer, corregir, actualizar o cancelar información personal que le afecta, mecanismos que se examinan a continuación. Esta última acción es analizada más específicamente en otro de los trabajos incluidos en el presente volumen.

Resguardos para el procesamiento computacional de información digital. Éstos pueden examinarse, ejemplarmente, a la luz de las normas españolas, en especial la Ley Orgánica 5/1992, sobre regulación del tratamiento automatizado de los datos de carácter personal (Lortad), que dio cumplimiento al mandato constitucional de "limitar el uso de la informática para garantizar el honor y la intimidad personal de los ciudadanos" (art. 18.4).

Esta ley contiene principios generales que rigen la recolección de información, destinados a garantizar tanto la veracidad de la información personal como la "congruencia y racionalidad" del uso de los datos, esto es, que ellos no sean utilizados sino para la finalidad con que fueron obtenidos⁴⁶.

⁴⁶ Francisco Fernández, "El Régimen Jurídico del Tratamiento Automatizado de los Datos de Carácter Personal en España", en *Ius et Praxis*, Universidad de Talca (1997), año 3, Nº 1, pp. 33-69. La exposición de los principios sigue básicamente esta obra (pp. 57-63).

La doctrina española ha distinguido seis grupos de principios orientadores de la protección a la información personal: consentimiento del afectado, tratamiento de datos sensibles, calidad de los datos, medidas de seguridad, deber de secreto y cesión de datos⁴⁷.

El principio básico en esa ley es exigir la obtención del consentimiento del afectado para el tratamiento computacional de sus datos, salvo en casos exceptuados: (a) recolección de datos de fuentes accesibles al público, (b) recolección para ejercer funciones propias de la administración pública o (c) recolección de datos cuando éstos 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" (Ley, art. 6º).

El principio del consentimiento se ve especialmente reforzado a propósito de la información sensible, pues en algunos casos (ideología, creencias religiosas) se exige el consentimiento expreso y por escrito del afectado y en otros (raza, salud, vida sexual) que exista una autorización legal expresa, pero en ambos casos se prohíben las bases de datos con ese solo objeto.

El principio de la calidad de los datos es el más amplio, pues comprende varios otros principios. El más importante, en mi opinión, es la exigencia de congruencia entre la finalidad perseguida y la información recabada (art. 4.1, 4.2). Además, la exigencia de que los datos sean verídicos, exactos y actuales (art. 4.3, 4.4), la prohibición de la recolección por medios fraudulentos, desleales o ilícitos (art. 4.2), la orden de que los datos sean almacenados de forma de poder acceder a ellos el interesado (art. 4.6) y, por último, el derecho a que los datos desaparezcan después del plazo establecido en la ley o en las relaciones contractuales entre el administrador de la base de datos y el afectado (art. 15.5).

En resguardo del principio de seguridad de los datos, la ley obliga a adoptar medidas para evitar la pérdida, alteración, tratamiento o acceso no autorizado (art. 9). La ley impone el deber de secreto profesional al responsable de la base de datos y a quienes intervengan en el tratamiento de datos de carácter personal (art. 10).

⁴⁷ Fernández, op. cit., pp. 57-63.

2. DERECHOS DE LAS PERSONAS

Los derechos de las personas son típicamente de cuatro clases: derecho a no ser valorado únicamente en datos automatizados, derecho a la información, derecho de acceso y derecho de rectificación y cancelación, que son desarrollados en este mismo volumen por el profesor Hernán Corral al tratar del *habeas data*.

3. RESPONSABILIDADES

Existen básicamente dos sistemas de responsabilidad de los administradores de las bases de datos: el sistema tradicional de responsabilidad por culpa o falta de diligencia y el sistema de responsabilidad estricta u objetiva.

Uno de los avances de la cuarta generación de leyes de protección de información digital fue establecer precisamente reglas sobre responsabilidad objetiva de los administradores (por ejemplo, como la reforma a la ley alemana de 1990), pero otras leyes, como la Lortad española, de 1992, mantienen un sistema de responsabilidad por culpa, aunque en ciertas circunstancias los deberes de vigilancia y cuidado son más estrictos (en protección de datos sensibles, por ejemplo).

4. PLAZOS

En la ley española (Lortad) no se distingue, respecto a información comercial, entre exigibilidad y pago o prescripción. La regla es que cuando la información sobre la solvencia económica sea adversa, no puede referirse a más de 6 años.

5. ORGANISMOS FISCALIZADORES

En España existe la "Agencia de Protección de Datos", creada por la Lortad, de 1992, un organismo dotado de personalidad jurídica, que actúa con plena independencia de la Administración Pública en el ejercicio de sus funciones. Le corresponde velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, especialmente en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.

En Francia, por otra parte, existe la "Comisión Nacional de la Informática y las Libertades", que está encargada de velar por la

observancia de la ley, especialmente informando a las personas interesadas acerca de sus derechos y obligaciones, consultándolas y vigilando la aplicación de la informática al tratamiento de informaciones nominativas.

6. ACCIONES ADMINISTRATIVAS Y PROCESALES

La principal acción que tienen los titulares de los datos personales es la acción de *habeas data*, que cumple variados propósitos, y que en algunos ordenamientos jurídicos ha obtenido reconocimiento constitucional.

Además, los titulares de la información tienen, en determinados casos, acción de responsabilidad por los perjuicios causados, la que ha tenido una tendencia a hacerse más objetiva, de tal manera que no debe probarse culpa o negligencia, bastando la relación de causalidad.

Por último, también existen acciones infraccionales, por incumplimiento de las reglas legales sobre protección de datos personales, que en el caso de la ley española pueden llegar como máximo a 100 millones de pesetas (equivalente a \$ 300 millones, aproximadamente).

V. LA NUEVA LEY CHILENA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LEY N° 19.628) EN LA PERSPECTIVA DEL DERECHO COMPARADO

1. INTERPRETACIÓN E INTEGRACIÓN

La nueva ley de datos personales ha tenido en consideración básicamente modelos legales comparados de España, Francia y Gran Bretaña, así como la experiencia acumulada en Chile, desde 1928, respecto a la publicación de antecedentes comerciales, en medios impresos (Boletín de la Cámara de Comercio de Santiago), primero, y en medios computacionales, posteriormente (informes de Dicom, filial de la empresa americana Equifax, una de las firmas más grandes del mundo en procesamiento y comercialización de información digital).

Aun cuando nació como un proyecto de ley mucho más ambicioso, que perseguía proteger la vida privada en prácticamente todos sus aspectos, la ley chilena recientemente aprobada se refiere específicamente a la "protección de datos personales". Así se expli-

ca la confusión que quedó finalmente –por un defecto de técnica legislativa– entre los dos títulos que tiene la ley, uno muy amplio y el otro mucho más restringido.

La historia fidedigna del establecimiento de la ley muestra que el proyecto fue discutido en el Congreso durante más de 6 años, iniciándose su tramitación el 5 de enero de 1993, mediante una moción presentada por el entonces senador Eugenio Cantuarias, que proponía la dictación de una “Ley sobre Protección Civil de la Vida Privada”.

El concepto de “vida privada de las personas” que empleaba el proyecto original comprendía, entre otros, los siguientes derechos: (1) a la propia imagen; (2) a la intimidad personal y familiar; (3) al anonimato y reserva; (4) a una vida tranquila, sin hostigamientos ni perturbaciones, y (5) a la inviolabilidad del hogar y de toda forma de comunicaciones privadas (artículo segundo)⁴⁸.

En cuanto a sus fuentes, dicho proyecto se basaba fundamentalmente en: (1) la ley orgánica N°1, de 5 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, de España; (2) la ley 78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades, de Francia; (3) la ley de 12 de junio de 1984, sobre protección de datos, de Gran Bretaña; (4) la ley N° 48, de 9 de junio de 1978, sobre registros de datos personales, de Noruega⁴⁹.

Sin embargo, durante su tramitación, el proyecto original fue reducido significativamente, siendo aprobado, en definitiva, sólo respecto a uno de los aspectos de la vida privada: la protección de datos personales o datos digitales (aun cuando también incluye datos en ficheros manuales, con el tiempo éstos han perdido importancia)⁵⁰.

Vale la pena destacar que durante la tramitación de la ley, un informe de la Cámara de Diputados definió la *intimidad* como “el entorno inmediato y los aspectos más reservados de la vida privada y de la propia persona que todo individuo tiene derecho a mante-

⁴⁸ Diario de Sesiones del Senado, sesión 20 Ordinaria, de 5.1.93, página 3084.

⁴⁹ Además, el proyecto original reconocía como fuentes: (1) el artículo 1071 bis del Código Civil Argentino, y (2) el artículo 9 del Código Civil francés.

⁵⁰ Para estos efectos, la Cámara de Diputados encargó a los diputados José Antonio Viera-Gallo y Luis Valentín Ferrada, previa consulta y autorización del senador Cantuarias, que elaboraran un nuevo proyecto (Informe de la Comisión de Constitución, Legislación y Justicia, de 20.5.96, Boletín 896-07 (S)).

ner fuera de toda intromisión". Asimismo, el *derecho a la intimidad* fue definido por ese mismo órgano como "el reconocimiento de que el concepto amplio de libertad exige que cada persona tenga un ámbito de desarrollo y expresión"⁵¹.

Una ley como ésta es un caso paradigmático de aplicación del derecho comparado como fuente material de derecho en nuestro sistema legal. En efecto, en atención a la ausencia de regulación legal previa respecto a la información digital (sólo existía la regulación de información comercial mediante impresos, contenida en un decreto supremo de 1928), el legislador se vio forzado a recurrir a la experiencia de otros países, tratando de recoger los elementos que más se asemejaran a la realidad nacional.

De esta manera, la tramitación de la ley da cuenta de que no sólo se tomaron de modelo las legislaciones extranjeras (en especial las de España, Francia y Gran Bretaña) para preparar el proyecto de ley original, sino que durante su discusión hubo frecuentes remisiones al derecho que rige estas materias también en Alemania, Suiza y Estados Unidos.

Así, por ejemplo, en una etapa de la redacción de la ley se estableció, siguiendo el modelo alemán, el derecho a la "autodeterminación informativa" de las personas respecto a sus datos personales, pero posteriormente se rechazó esta idea porque se estimó que esta doctrina no era pacífica en la propia Alemania, y el riesgo que podría generar de una interpretación patrimonialista, en cuanto induciría a las personas a pensar que tienen un derecho de propiedad sobre sus datos⁵².

En la misma tramitación de la ley hay referencias a la teoría suiza de las tres esferas (intimidad, privacidad y publicidad), así como al significado del concepto de *privacy* en el derecho norteamericano⁵³.

En definitiva, la nueva ley siguió en forma muy cercana la legislación alemana y española, pero especialmente esta última. Tanto es así que cuando se plantearon en una Sesión del Pleno de la Cámara de Diputados los "principios" que informaban el segundo proyecto de ley, se hizo mención exactamente a los mismos seis

⁵¹ Ídem nota 50, pág. 153.

⁵² Véase Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, recaído en el proyecto de ley, en tercer trámite, sobre protección de la vida privada (896-07), de 4 de agosto de 1998, página 2089.

⁵³ Ídem nota 52.

principios antes expuestos que rigen la ley española (consentimiento, datos especialmente protegidos, calidad de los datos, medidas de seguridad, deber de secreto y cesión de los datos)⁵⁴.

Por las razones expuestas, en casos en que se presente la necesidad de interpretar pasajes oscuros o dudosos de la ley, o en aquellos casos en que no exista norma precisa que regule la materia y en que el juez deba integrar la ley aún a falta de regla expresa, el derecho comparado y, especialmente, el modelo legal español cumplirán un papel insustituible en la aplicación de la nueva ley.

2. REFORMA

La nueva ley presenta la ventaja evidente de establecer por primera vez en nuestro país reglas y procedimientos de rango legal para proteger la intimidad de las personas ante las amenazas que les puede deparar el uso de información digital.

Con todo, analizada la nueva ley a la luz del derecho comparado, presenta desde ya, en mi opinión, insuficiencias que probablemente harán necesaria su reforma dentro de poco tiempo. El defecto principal de la nueva ley es que, aun cuando otorga mecanismos de protección novedosos en nuestro medio tales como el *habeas data*, pone a las personas en una situación de evidente desventaja y notorio desequilibrio frente a las empresas administradoras de bases de datos, como se ha comprobado en Europa, al menos por las siguientes cuatro razones:

2.1 Inexistencia de autoridad reguladora

La nueva ley, al no haber establecido una entidad autónoma con atribuciones y poderes para regular la gestión de las sociedades administradoras de bases de datos y solucionar algunos conflictos, como ha ocurrido en las experiencias europeas más exitosas (Alemania, España, Francia, etc.), obliga a los particulares a recurrir a los Tribunales de Justicia, lo que significa necesariamente alto costo para las víctimas y largo tiempo de espera, aun cuando se haya hecho un esfuerzo legislativo por abreviar los plazos.

⁵⁴ Véase intervención del diputado Gutenberg Martínez en la sesión 13ª de la Cámara de Diputados, del miércoles 5 de noviembre de 1997, págs. 29 a 31.

2.2 Dificultades de la responsabilidad por culpa

En segundo lugar, la nueva ley, al establecer la responsabilidad basada en la culpa del administrador o responsable de la base de datos, en lugar de un sistema de responsabilidad objetiva, pone de cargo de la víctima la carga onerosa y prácticamente imposible de acreditar esa culpa o negligencia.

2.3 Inexistencia de un registro de bases de datos privadas

En mi opinión, un tercer defecto de la ley es no haber creado un registro general de bases de datos que incluya bases privadas, lo que dificulta el ejercicio de sus derechos, especialmente a personas naturales.

2.4 Multas que no significan disuasivos reales

Por último, 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. Así, como la experiencia ha mostrado en Chile respecto a la ley de protección al consumidor, puede ocurrir que las administradoras de bases de datos evalúen que resulta más eficiente (en términos de gastos legales, tiempo y multa) pagar las sanciones que adecuarse efectivamente a la ley. La multa máxima en Chile, de 50 UTM, equivalente a \$ 2.500.000, es ridícula si se la compara con la multa máxima en España, que puede ascender a \$ 300 millones, lo que la convierte en un muy poderoso disuasivo.

